

23/11

SI

IN THE HON'BLE SUPREME COURT OF INDIA
CIVIL WRIT PETITION NO : 829 OF 2013
(UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA)

IN THE MATTER OF :

MR. S.G VOMBATKARE & ANR

.....

PETITIONERS

VS

UNION OF INDIA & ORS.

.....

RESPONDENTS

COUNTER AFFIDAVIT ON BEHALF OF RESPONDENT NO 3
(UIDAI)

PAPER BOOK

(VOLUME-II)

(FOR INDEX, KINDLY SEE INSIDE)

DS MAHRA

ADVOCATE ON RECORD FOR THE PETITIONER

INDEX

| Srl No. | <u>Particulars</u> | Pages |
|---------|--|------------|
| 1. | Copy of the UIDAI Strategy Overview - ANNEXURE R-1 | 66 to 109 |
| 2. | A short power point presentation on the security of the data - ANNEXURE R-2 | 110 to 113 |
| 3. | Copy of the relevant Report of the Planning Commission - ANNEXURE R-3. | 114 to 116 |
| 4. | Copy of the approval to Project of Unique Identification for BPL Families - ANNEXURE R-4. | 117 to 117 |
| 5. | Copy of "Strategic Vision on the UID Project" - ANNEXURE R-5 | 118 to 138 |
| 6. | Copy of the constitution and Terms of Reference of the EGoM - ANNEXURE R-6 | 139 to 139 |
| 7. | Copy of the Minutes of the Meeting dated 27.11.2007 - ANNEXURE R-7 | 140 to 146 |
| 8. | Copy of the Minutes of the Meeting dated 28.1.2008 - ANNEXURE R-8 | 147 to 154 |
| 9. | Copy of the Minutes of the Meeting dated | 155 to 163 |

| | | |
|-----|--|-------------------|
| | 07.08.2008 - ANNEXURE R-9 | |
| 10. | Copy of the Minutes of the Meeting dated 04.11.2008 - ANNEXURE R-10 | 164 to 173 |
| 11. | Copy of the letter dated 22.1.2009, related to the decision to constitute UIDAI - ANNEXURE R-11 | 174 to 174 |
| 12. | Copy of the Gazette Notification dated 28.01.2009, constituting the UIDAI - ANNEXURE R-12 | 175 to 180 |
| 13. | Copy of the Notification dated 22 nd October, 2009, constituting the Cabinet Committee on UIDAI - ANNEXURE R-13. | 181 to 182 |
| 14. | A copy of the Direct Benefit Transfer Scheme notification dated 26 th December, 2012 - ANNEXURE R-16. | 183 to 184 |
| 15. | Copy of the "Biometric Design Standards for UID Applications" - ANNEXURE R-17. | 185 to 251 |
| 16. | Copy of the "UID Enrolment - Proof of Concept Report" - ANNEXURE R-17. | 252 to 283 |



सत्यमेव जयते

UIDAI STRATEGY OVERVIEW

CREATING A UNIQUE IDENTITY NUMBER FOR
EVERY RESIDENT IN INDIA



Unique Identification Authority of India (UIDAI)
Planning Commission, Govt. of India
April, 2010

CONTENTS

| | |
|---|-----------|
| Executive Summary | 1 |
| 1 Introduction and historical background | 6 |
| 1.1 Historical background and evolution of the UIDAI project | 6 |
| 1.2 The UIDAI Approach | 9 |
| 2 The UIDAI implementation model | 10 |
| 2.1 The Central Identities Data Repository (CIDR) | 10 |
| 2.2 The Unique Identity Number | 10 |
| 2.3 The Unique ID agencies | 11 |
| 2.4 Setting standards on demographic data and biometrics | 12 |
| 3 Enrolment into the UID system | 14 |
| 3.1 The enrolment process | 14 |
| 3.2 Enrolment strategy in rural and urban India | 16 |
| 3.3 A focused effort to enrol the poor and hard to reach groups | 17 |
| 3.4 Enrolment cost | 19 |
| 3.5 Ensuring clean enrolment data from registrars | 20 |
| 3.6 Updating UID details | 20 |
| 3.7 Reaching critical mass in enrolments | 21 |
| 3.8 Tracking enrolments across the country | 22 |
| 3.9 Reaching a sustainable steady state in enrolments | 23 |
| 4 Ensuring strong authentication and what it means for the UIDAI | 25 |
| 4.1 Enabling UID adoption for authentication | 25 |
| 4.2 Types of authentication | 26 |
| 4.3 Authentication and the UIDAI revenue model | 27 |
| 5 Legal framework | 30 |
| 6 Data security and fraud | 33 |
| 6.1 Protecting personal information of residents | 33 |
| 6.2 Fraud scenarios | 34 |
| 7 Technology architecture of the UIDAI | 35 |
| 7.1 System architecture | 35 |
| 8 Project execution | 37 |
| 8.1 Addressing challenges of scale | 37 |
| 9 Project risks | 38 |
| 10 UID-enabled micropayment architecture | 39 |
| 10.1 Features of UID-enabled micropayments | 40 |
| 10.2 Benefits | 41 |
| 10.3 Conclusion | 42 |

Executive Summary

Overview

In India, an inability to prove identity is one of the biggest barriers preventing the poor from accessing benefits and subsidies. Public as well as private sector agencies across the country typically require proof of identity before providing individuals with services. But till date, there remains no nationally accepted, verified identity number that both residents and agencies can use with ease and confidence.

As a result, every time an individual tries to access a benefit or service, they must undergo a full cycle of identity verification. Different service providers also often have different requirements in the documents they demand, the forms that require filling out, and the information they collect on the individual.

Such duplication of effort and 'identity silos' increase overall costs of identification, and cause extreme inconvenience to the individual. This approach is especially unfair to India's poor and underprivileged residents, who usually lack identity documentation, and find it difficult to meet the costs of multiple verification processes.

There are clearly, immense benefits from a mechanism that uniquely identifies a person, and ensures instant identity verification. The need to prove identity only once will bring down transaction costs for the poor. A clear identity number would also transform the delivery of social welfare programs by making them more inclusive of communities now cut off from such benefits due to their lack of identification. It would enable the government to shift from indirect to direct benefits, and help verify whether the intended beneficiaries actually receive funds/subsidies.

A single, universal identity number will also be transformational in eliminating fraud and duplicate identities, since individuals will no longer be able to represent

themselves differently to different agencies. This will result in significant savings to the state exchequer.

The UIDAI - evolving an approach to identity

The Government of India undertook an effort to provide a clear identity to residents first in 1993, with the issue of photo identity cards by the Election Commission. Subsequently in 2003, the Government approved the Multipurpose National Identity Card (MNIC).

The Unique Identification Authority of India (UIDAI) was established in January 2009, as an attached office to the Planning Commission. The purpose of the UIDAI is to issue a unique identification number (UID) to all Indian residents that is (a) robust enough to eliminate duplicate and fake identities, and (b) can be verified and authenticated in an easy, cost-effective way. The UIDAI's approach will keep in mind the learnings from the government's previous efforts at issuing identity.

The UIDAI will be created as a statutory body under a separate legislation to fulfill its objectives. The law will also stipulate rules, regulations, processes and protocols to be followed by different agencies partnering with the UIDAI in issuing and verifying unique identity numbers.

Features of the UIDAI model

The Unique Identification number (UID) will only provide identity: The UIDAI's purview will be limited to the issue of unique identification numbers linked to a person's demographic and biometric information. The UID will only guarantee identity, not rights, benefits or entitlements.

The UID will prove identity, not citizenship: All residents in the country can be issued a unique ID. The UID is proof of identity and does not confer citizenship.

A pro-poor approach: The UIDAI envisions full enrolment of residents, with a focus on enrolling India's poor and underprivileged communities. The Registrars that the UIDAI plans to partner with – the NREGA, RSBY, and PDS – will help bring large numbers of the poor and underprivileged into the UID system. The UID method of authentication will also improve service delivery for the poor.

Enrolment of residents with proper verification: Existing identity databases in India are fraught with problems of fraud and duplicate/ghost beneficiaries. To prevent this from seeping into the UIDAI database, the UIDAI plans to enrol residents into its database with proper verification of their demographic and biometric information. This will ensure that the data collected is clean from the start of the program.

However, much of the poor and underserved population lack identity documents and the UID may be the first form of identification they have access to. The UIDAI will ensure that the Know Your Resident (KYR) standards don't become a barrier for enrolling the poor, and will devise suitable procedures to ensure their inclusion without compromising the integrity of the data.

A partnership model: The UIDAI approach leverages the existing infrastructure of government and private agencies across India. The UIDAI will be the regulatory authority managing a Central Identities Data Repository (CIDR), which will issue UIDs, update resident information, and authenticate the identity of residents as required.

In addition, the UIDAI will partner with agencies such as central and state departments and private sector agencies who will be 'Registrars' for the UIDAI. Registrars will process UID applications, and connect to the CIDR to de-duplicate resident information and receive UID numbers. These Registrars can either be enrollers, or will appoint agencies as enrollers, who will interface with people seeking UID numbers. The Authority will also partner with service providers for authentication.

The UIDAI will emphasize a flexible model for Registrars: The Registrars will retain significant flexibility in their processes, including issuing cards, pricing, expanding KYR (Know Your Resident) verification, collecting demographic data on residents for their specific requirements,

and in authentication. The UIDAI will provide standards to enable Registrars maintain uniformity in collecting certain demographic and biometric information, and in basic KYR. These standards have been finalized by the Demographic Data Standards and Verification Procedures Committee and Biometric Standards Committees which was constituted by the UIDAI constituted.

Enrolment will not be mandated: The UIDAI approach will be a demand-driven one, where the benefits and services that are linked to the UID will ensure demand for the number. This will not however, preclude governments or Registrars from mandating enrolment.

The UIDAI will issue a number, not a card: The UIDAI's role is limited to issuing the number. This number may be printed on the document/card that is issued by the Registrar.

The number will not contain intelligence: Loading intelligence into identity numbers makes them susceptible to fraud and theft. The UID will be a random number.

The UIDAI will only collect basic information on the resident: The UIDAI will seek the following demographic and biometric information in order to issue a UID number:

- Name
- Date of birth
- Gender
- Father's/ Husband's/ Guardian's name and UID number (optional for adult residents)
- Mother's/ Wife's/ Guardian's name and UID number (optional for adult residents)
- Introducer's name and UID number (in case of lack of documents)
- Address
- All ten fingerprints, photograph and both iris scans

Process to ensure no duplicates: Registrars will send the applicant's data to the CIDR for de-duplication. The CIDR will perform a search on key demographic fields and on the biometrics for each new enrolment, to ensure that no duplicates exist.

The incentives in the UID system are aligned towards a self-cleaning mechanism. The existing patchwork of multiple databases in India gives individuals the incentive to provide different personal information to different agencies. Since de-duplication in the UID system ensures that residents have only one chance to be in the database, individuals will provide accurate data. This incentive will become especially powerful as benefits and entitlements are linked to the UID.

Online authentication: The UIDAI will offer a strong form of online authentication, where agencies can compare demographic and biometric information of the resident with the record stored in the central database. The Authority will support Registrars and agencies in adopting the UID authentication process, and will help define the infrastructure and processes they need.

The UIDAI will not share resident data: The UIDAI envisions a balance between 'privacy and purpose' when it comes to the information it collects on residents. The agencies may store the information of residents they enrol if they are authorized to do so, but they will not have access to the information in the UID database. The UIDAI will answer requests to authenticate identity only through a 'Yes' or 'No' response

Technology will undergird the UIDAI system: Technology systems will have a major role across the UIDAI infrastructure. The UID database will be stored on a central server. Enrolment of the resident will be computerized, and information exchange between Registrars and the CIDR will be over a network. Authentication of the resident will be online. The Authority will also put systems in place for the security and safety of information.

Benefits

For residents: The UID will become the single source of identity verification. Once residents enrol, they can use the number multiple times – they would be spared the hassle of repeatedly providing supporting identity documents each time they wish to access services such as obtaining a bank account, passport, driving license, and so on.

By providing a clear proof of identity, the UID will also facilitate entry for poor and underprivileged residents into the formal banking system, and the opportunity to avail services provided by the government and the private sector. The UID will also give migrants mobility of identity.

For Registrars and enrollers: The UIDAI will only enrol residents after de-duplicating their records. This will help Registrars clean out duplicates from their databases, enabling significant efficiencies and cost savings. For Registrars focused on cost, the UIDAI's verification processes will ensure lower KYR costs. For Registrars focused on social goals, a reliable identification number will enable them to broaden their reach into groups that till now, have been difficult to authenticate. The strong authentication that the UID number offers will improve services, leading to better resident satisfaction.

For Governments: Eliminating duplication under various schemes is expected to save substantial money for the government exchequer. It will also provide governments with accurate data on residents, enable direct benefit programs, and allow government departments to coordinate investments and share information.

Revenue Model

By providing identity authentication, the UIDAI will be taking on a process that costs agencies and service providers hundreds of crores every year. The Authority will evolve suitable policies on the issue of charging a fee for its authentication services, which will offset its long-term costs. Registrars and service providers will also be able to charge for the cards they issue residents with the UID number. Such pricing will be within UIDAI guidelines.

Timelines

The UIDAI will start issuing UIDs between August 2010 and February 2011, and plans to cover 600 million people within 4 years from the start of the issuing of the first set of UIDs. This can be accelerated if more Registrars partner with the UIDAI for both enrolment and authentication. The adoption of UIDs is expected to gain momentum with time, as the number establishes itself as the most accepted identity proof in the country.

Conclusion

India will be the first country to implement a biometric-based unique ID system for its residents on such a large scale. The UID will serve as a universal proof of identity, allowing residents to prove their identity anywhere in the country. It will give the government a clear view of India's population, enabling it to target and deliver services effectively, achieve greater returns on social investments, and monitor money and resource flows across the country.

The timing of this initiative is encouraging – the creation of the UIDAI coincides with growing social investment in India, a shift in focus to direct benefits, and with the spread of IT and mobile phones, which has made the public receptive to technology-based solutions. The UIDAI is committed to making this project a success. An initiative of this magnitude will also require the active participation of central, state and local governments, as well as public and private sector agencies across the country. With their support, the project will help realize a larger vision of inclusion and development for India.

Introduction and historical background

A crucial factor that determines an individual's well-being in a country is whether their identity is recognized in the eyes of the government. Weak identity limits the power of the country's residents when it comes to claiming basic political and economic rights. The lack of identity is especially detrimental for the poor and the underprivileged, the people who live in India's "social, political and economic periphery". Agencies in both the public and private sector in India usually require a clear proof of identity to provide services. Since the poor often lack such documentation, they face enormous barriers in accessing benefits and subsidies.

For governments and individuals alike, strong identity for residents has real economic value. While weak identity systems cause the individual to miss out on benefits and services, it also makes it difficult for the government to account for money and resource flows across a country. In addition, it complicates government efforts to account for residents during emergencies and security threats.

However in India, the goal of issuing a universally used, unique identity number to each resident poses a significant challenge. A project of this scale has not been attempted anywhere in the world, and requires an innovative model, distinct from what we have witnessed in identity systems so far anywhere in the world.

1.1 Historical background and evolution of the UIDAI project

The Unique identification project was initially conceived by the Planning Commission as an initiative that would provide a clear and unique identity number for each resident across the country and would be used primarily as the basis for efficient delivery of welfare services. It would also act as a tool for effective monitoring of various programs and schemes of the Government.

The concept of unique identification was first discussed and worked upon since 2006 when administrative approval for the project – "Unique ID for BPL families" was given on March 3rd, 2006 by the Department of Information Technology, Ministry of Communications and Information Technology. This project was to be implemented by the NIC over a period of 12 months. Subsequently, a Processes Committee to suggest processes for updation, modification, addition and deletion of data fields from the core data base to be created under the Unique ID for BPL families Project was set up on July 3rd, 2006.

A "Strategic Vision on the UID Project" was prepared and submitted to this Committee. It envisaged the close linkage that the UID would have to the electoral database. The Committee also appreciated the need of a UID Authority to be created by an executive order under the aegis of the Planning Commission to ensure a pan-departmental and neutral identity for the Authority and at the same time enable a focused approach to attaining the goals set for the XI Plan. The Seventh

Meeting of the Process Committee on 30th August 2007 decided to furnish to the Planning Commission a detailed proposal based on the resource model for seeking its "in principle" approval.

At the same time, the Registrar General of India was engaged in the creation of the National Population Registrar and issuance of Multi-purpose National Identity Cards to citizens of India.

Therefore, it was decided, with the approval of the Prime Minister, to constitute an Empowered Group of Ministers (EGoM) to collate the two schemes – the National Population Register under the Citizenship Act, 1955 and the Unique Identification Number project of the Department of Information Technology. The EGoM was also empowered to look into the methodology and specific milestones for early and effective completion of the Project and take a final view on these. The EGoM was constituted on December 4th, 2006.

The **first meeting of the EGoM** was held on November 27th, 2007. It recognised the need for creating an identity related resident database, regardless of whether the database is created based on a de-novo collection of individual data or is based on already existing data such as the voter list. It also recognised that there is a crucial and imperative need to identify and establish an institutional mechanism that will "own" the database and will be responsible for its maintenance and updating on an ongoing basis, post its creation.

The **second meeting of the EGoM** was held on January 28th, 2008. It decided on the strategy for the collation of NPR and UID. Inter-alia, the proposal to establish UID Authority under the Planning Commission was approved.

The **third meeting of the EGoM** was held on August 7th, 2008. The Planning Commission had placed before the EGoM a detailed proposal for setting up the UIDAI. The meeting decided that certain issues raised by the members with relation to the UIDAI would need to be examined by an official level committee. It referred the matter to a Committee of Secretaries to examine and give its recommendations to the EGoM to facilitate a final decision.

Subsequent to the Committee of Secretaries recommendations, the **fourth meeting of the EGoM** was held on November 4th, 2008. The recommendations of the Committee of Secretaries was presented to the EGoM and the following decisions were taken:

- a) Initially the UIDAI may be notified as an executive authority, and investing it with statutory authority could be taken up for consideration later at an appropriate time.
- b) UIDAI may limit its activities to the creation of the initial database from the electoral roll/EPIC data. UIDAI may however additionally issue instructions to agencies that undertake creation of databases to ensure standardization of data elements.
- c) UIDAI will take its own decision as to how to build the database.
- d) UIDAI would be anchored in the Planning Commission for five years after which a view would be taken as to where the UIDAI would be located within Government.

- e) Constitution of the UIDAI with a core team of 10 personnel at the central level and directed the Planning Commission to separately place a detailed proposal with the complete structure, rest of staff and organizational structure of UIDAI before the Cabinet Secretary for his consideration prior to seeking approval under normal procedure through the DoE/CCEA.
- f) Approval to the constitution of the State UID Authorities simultaneously with the Central UIDAI with a core team of 3 personnel.
- g) December 2009 was given as the target date for UID to be made available for usage by an initial set of authorized users.
- h) Prior to seeking approval for the complete organizational structure and full component of staff through DoE and CCEA as per existing procedure, the Cabinet Secretary should convene a meeting to finalize the detailed organizational structure, staff and other requirements.

1.1. Subsequently, on January 22nd, 2009 the Cabinet Secretary in pursuance of the decisions of the Empowered Group of Ministers considered the proposal submitted by the Department of Information Technology regarding the governance structure and recommended that

- a) The notification for constitution of the UIDAI should be issued immediately.
- b) A High Level Advisory, Monitoring and Review Committee headed by Deputy Chairman, Planning Commission to be constituted to oversee the work of the authority.
- c) A Member, Planning Commission or the Secretary, Planning Commission may be also assigned the task of looking after the work proposed of the Chief UID Commissioner.
- d) Core Team to be put in place.

In pursuance of the Empowered group of Ministers' fourth meeting dated November 4th, 2008, the **Unique Identification Authority of India** was constituted and notified by the Planning Commission on January 28th, 2009 as an attached office under the aegis of Planning Commission with an initial core team of 115 officials. The role and responsibilities of the UIDAI was laid down in this notification. The UIDAI was given the responsibility to lay down plan and policies to implement UID scheme, and shall own and operate the UID database and be responsible for its updation and maintenance on an ongoing basis.

Subsequently on July 2nd, 2009 Shri Nandan Nilekani was appointed as the Chairman of the UIDAI. Shri Nilekani assumed charge on 23rd July, 2009 and since then the UIDAI has started functioning.

The Prime Minister's Council on UID Authority was constituted on 30th July, 2009 and its first meeting had taken place on 12th August, 2009. The Council endorsed the broad approach submitted by the UIDAI.

Subsequently, the Government constituted a **Cabinet Committee on Unique Identification**

Authority of India vide its order no 1/11/6/2009 dated 22nd October, 2009. The functions of this Committee, as per this notification are: All issues relating to the Unique identification Authority of India including its organisation, plans, policies, programmes, schemes, funding and methodology to be adopted for achieving the objectives of that Authority.

1.2 The UIDAI approach

In 2007, the Planning Commission had recommended an approach to issuing unique identification numbers, where the enrolment into a Unique Identification (UID) database could be speeded up by using existing resident records in the databases of the Election Commission, PAN etc. This approach would speed up enrolment for those residents present in one of the aforementioned databases. These databases however, may contain inaccuracies.

The model envisioned by the Unique Identification Authority of India (UIDAI) takes into account the inputs of the Planning Commission, as well as learnings from the previous approaches to identity. The detailed approach and the model of implementation is explained in subsequent chapters.

2

The UIDAI Implementation Model

The model that the UIDAI envisions will have the reach and flexibility to enrol residents across the country.

The UIDAI, as a statutory body, will be responsible for creating, administering and enforcing policy. The UIDAI will prescribe guidelines on the biometric technology, the various processes around enrolment, and verification procedures to be followed to enroll into the UID system. The UIDAI will also design and create the institutional microstructure to effectively implement the policy. This will include a Central ID Data Repository (CIDR), which will manage the central system, and a network of Registrars who will establish resident touch points through Enrolling Agencies.

2.1 The Central Identities Data Repository (CIDR)

The CIDR will be the central data repository, and will function as a Managed Service Provider. It will implement the core services around the UID – it will store resident records, issue unique identification numbers, and verify, authenticate and amend resident data.

The CIDR will only hold the minimum information required to identify the resident and ensure no duplicates. This will include:

2.2 The Unique Identity Number

The Unique ID or UID will be a numeric that is unique across all 1.2 billion residents in India.

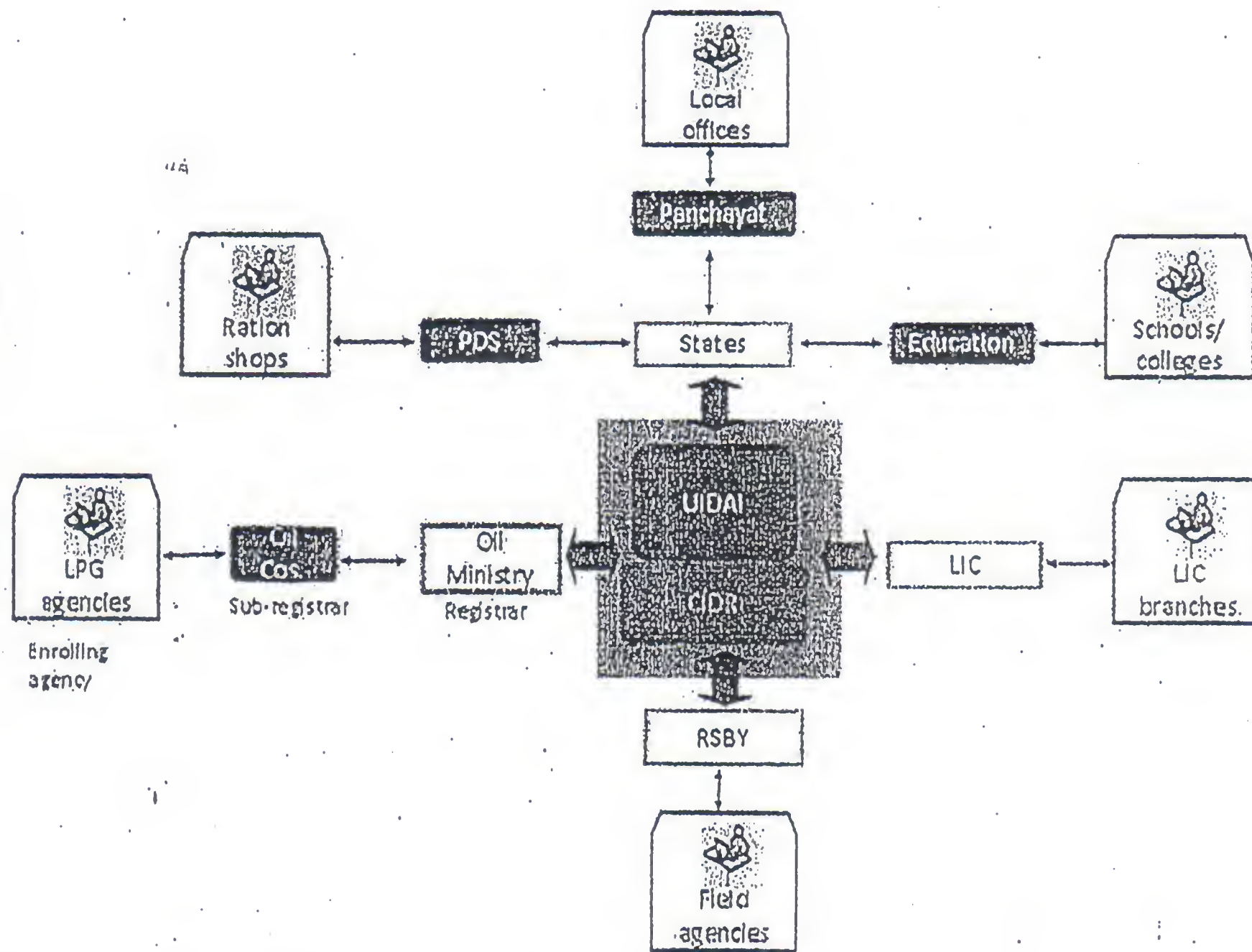
The UID number will not contain intelligence. In older identity systems, it was customary to load the ID number with information related to the date of birth, as well as the location of the person. However this makes the number susceptible to fraud and theft, and migration of the resident quickly makes location details out of date. The UID will be a random number.

The UIDAI will also be collecting the following data fields and biometrics for issuing a UID:

- Name
- Date of birth
- Gender
- Father's/ Husband's/ Guardian's name and UID (optional for adult residents)
- Mother's/ Wife's/ Guardian's name and UID (optional for adult residents)
- Introducer's name and UID (in case of lack of documents)
- Address
- All ten finger prints, photograph and both iris scans

2.3 The Unique ID agencies

The UIDAI will partner with a variety of agencies and service providers to enrol residents for UID numbers and verify their identity.



The structure of these UID agencies will be as follows:

Registrars – Registrars will be State governments or central government agencies such as the Oil Ministry and LIC. Registrars may also be private sector participants such as banks and insurance firms.

The UIDAI will enter into memorandum of understandings' (MoUs) with individual Registrars, and enable their on-boarding into the UID system. The Registrars will need to make changes to their processes to be UID-ready. The UIDAI will support them in this, and in linking to the CIDR, connecting to the UID system, and adding UID fields to their databases.

The Registrar will take on the responsibility of ensuring that clean and correct data flows into the CIDR. Their key role in the system will be in aggregating enrolments from sub-registrars and enrolling agencies and forwarding it to the CIDR. Each Registrar will adopt UIDAI standards in the technology used for biometrics, as well as in collecting and verifying resident information, and submitting to audits.

The UIDAI will also enter into agreements with some Registrars for using the CIDR solely for authentication purposes. The service providers who will adopt the UID system for identity authentication during service delivery will follow certain processes and standards, and may need to re-engineer their internal processes.

Sub-Registrars - These will be the departments/entities that report to a specific Registrar. For instance, the line departments of the state government such as the RDPR (Rural Development and Panchayati Raj) department would be sub-registrars to the state government Registrar.

Enrolling Agencies - Enrolling agencies will directly interact with and enrol residents into the CIDR. For example, the hospital where a baby is born would be the 'enrolling agency' for the baby's UID, and would report to the municipality sub-registrar.

Outreach Groups - The UIDAI along with the Registrars will also partner with civil society groups and community networks which will promote the UID number and provide information on enrolment for hard to reach and marginalised populations.

2.4 Setting standards on demographic data and biometrics

The UIDAI's approach relies on the uniformity of standards in certain vital areas of operation. The Demographic data fields and verification procedure in the UID system as well as the Biometric standards to be utilized need to be standardized across the country and across the various registrars in the UID system. This is a sine qua non for the operability of the system. Hence, the UIDAI established two Committees to look into the issue of standards.

Committee on Demographic Data Standards and Verification Procedures

The UIDAI had constituted a Committee headed by Mr. N. Vittal, former CVC on 9th October 2009 to go into the question as to what demographic details should be collected from the residents for assigning of unique IDs. The Committee was also to go into the question as to what should be the process of verification of the residents at the time of their enrolment into the UID system. The mandate of the Committee was crucial because it is necessary to ensure that the integrity and correctness of the data is not compromised while ensuring that the process of verification is non-harassing to individuals. The Committee was mandated to give its report within 90 days of its constitution. However, it submitted its report on 9th December 2009, well before the ninety days' period given to it. The Report of the Committee has been accepted by the Authority. The Committee recommended the following data fields : Name, Date of birth, Gender, Father's/ Husband's/ Guardian's name and UID (optional for adult residents), Mother's/ Wife's/ Guardian's name and UID (optional for adult residents), Introducer's name and UID (in case of lack of documents) and Address. It has also specified the verification process which broadly falls into three categories (i) Document-based, (ii) Introducer-based (in case of lack of documents) and (iii) Community-based verifications, a process which will be followed during the creation of NPR. The Report of the Vittal Committee is available at www.uidai.gov.in

Committee on Biometric Standards

As biometric attributes of the residents are going to be used as the basic signature for de-duplication and to ensure uniqueness, it is necessary to go into the question as to what should be the type and specifications of biometrics to be collected at the time of enrolment. Therefore, a Biometrics Standards Committee, under the Chairmanship of the Director General of NIC, Dr. BK Gairola was constituted by the Authority on 29th September, 2009. This Committee was also expected to give its report within 90 days of its constitution. The Report was submitted on 7th January, 2010. The UIDAI has examined their Report and has accepted the standards for various biometric attributes as recommended by the committee as also various other recommendations related to collection of biometrics and their quality. The UIDAI has also decided that the face, all ten finger prints and both iris scans should be collected at the time of capturing the demographic and biometric details of a resident. This will be able to ensure uniqueness of the IDs at a scale of 1.2 billion residents. The report of the biometric committee is also available at www.uidai.gov.in

The UIDAI was declared as an Apex body to set standards in the areas of biometric and demographic data standards by the Prime Minister's Council of UIDAI. Now that both these standards have been finalized by the UIDAI, these standards/specifications, processes and systems will be used by all the registrars to for enrolment of the residents into the UID system.

3

Enrolment into the UID system

A critical aspect of the UID enrolment process is that enrolment will not be through a mandate, but will be demand driven. The momentum for the UID will come from residents enrolling in order to access the benefits and services associated with it.

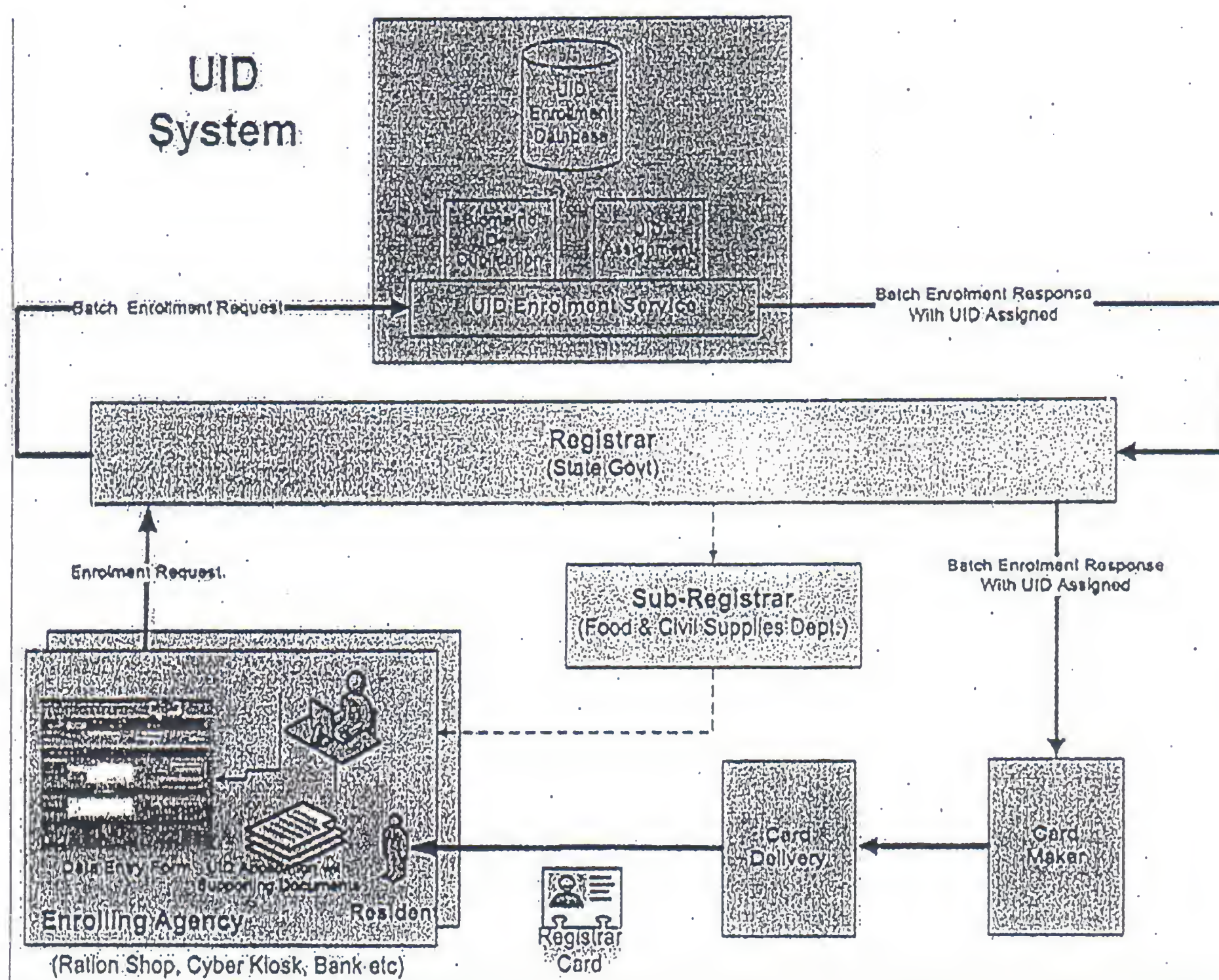
The basic advantage of the UID that can drive this demand, which will be communicated while promoting enrolment, is that the UID will be one number, which can be used to prove identity for life. Once the resident gets the unique ID, it may be accepted as identity proof across service providers.

3.1 The enrolment process

The enrolment process for the UID number will begin with a resident submitting his/her information to the enrolling agency with supporting documents. This information will be verified according to the prescribed verification procedure as per the DDSVP Committee Report. To make sure the poor are not excluded, the UIDAI has prescribed guidelines for applicants without documents.

Once the enroller verifies the resident's information, it will submit the application request – either singly or in batches – through the Registrar to the CIDR. The CIDR will then run a de-duplication check, comparing the resident's biometric and demographic information to the records in the database to ensure that the resident is not already enrolled.

Since de-duplication also compares biometric records, it would catch individuals enrolling with a different set of demographic details. The fact that the UID system is both de-duplicated and universal will discourage residents from giving incorrect data at the time of enrolment.



Issuing the UID number

Once the UID number is assigned, the UIDAI will forward the resident a letter which contains his/her registered demographic and biometric details. This letter may also have a tearaway portion which has the UID number, name, photograph and a 2D barcode of the finger print minutiae digest. If there are any mistakes in the demographic details, the resident can contact the relevant Registrar/enrolling agency as per a prescribed procedure.

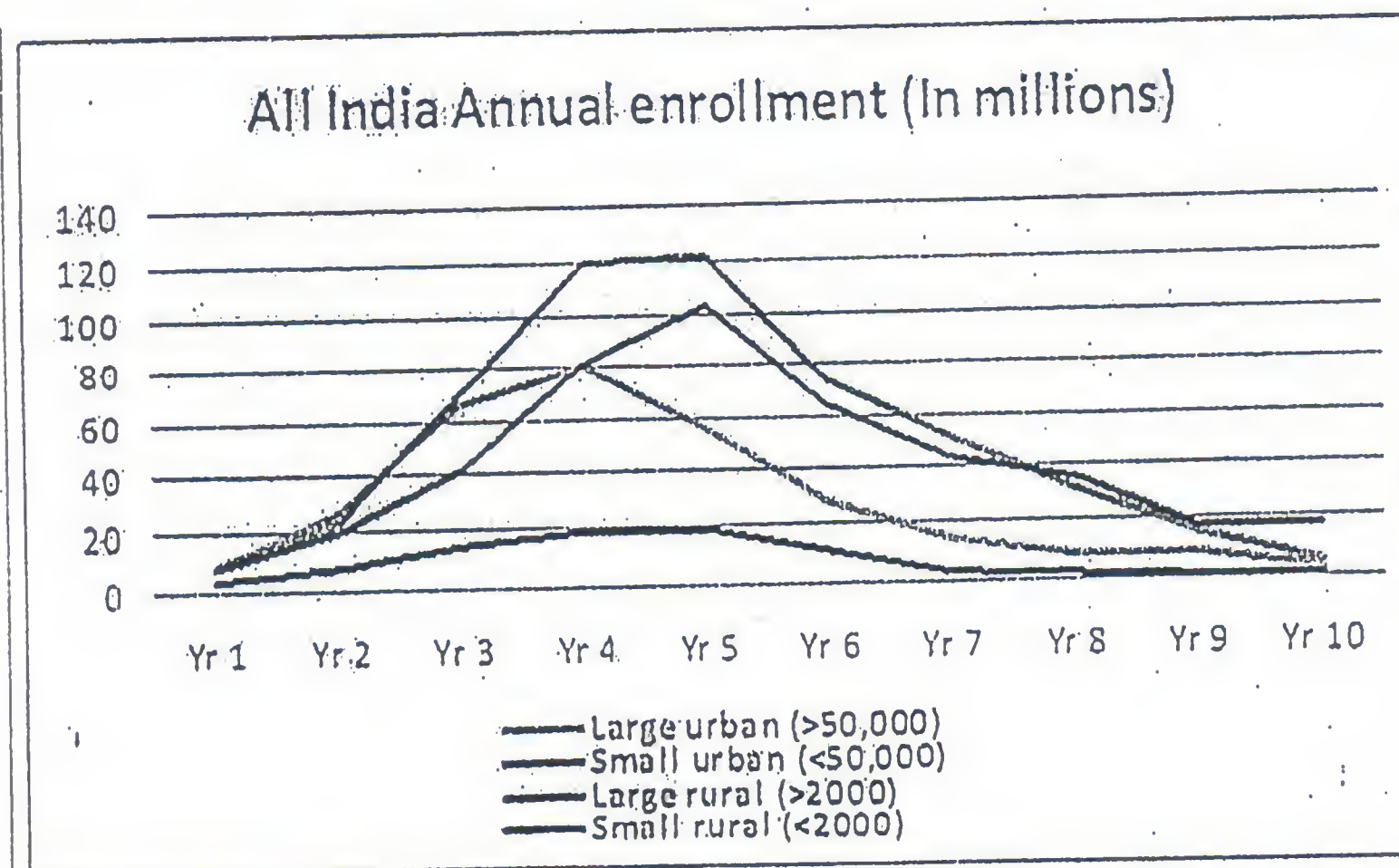
If the Registrar issues a card to the resident, the UIDAI will recommend that the card contain the UID number, name and photograph. They will be free to add any more information related to their services (such as Customer ID by bank). They will also be free to print/ store the biometric collected from the applicant on the issued card. If more registrars store such biometric information in a single card format, the cards will become interoperable for offline verification. But the UIDAI will not insist on, audit or enforce this.

All data entry that the enrolling agencies take up on behalf of the Registrars will be done in English. It can then be converted into the local language using standard transliteration software, and verified for accuracy by the Registrar. The letter the UIDAI sends the resident will consequently

contain all demographic details in English as well as the local language of the state in which the resident resides. In this regard, the UIDAI will follow the precedent set by the Election Commission of India.

3.2 Enrolment strategy in rural and urban India

The approach of the UIDAI to enrolment will be a pro-rural/pro-poor one. The Registrars targeted for rural India - the NREGA, PDS, Social security pensions - will be government agencies with large rural networks and significant bases among the poor. As a result, the UIDAI expects initial enrolment to be fairly rapid in both large and small rural areas.



The enrolment strategy for urban India will include organizations which dominate services for urban residents, such as LIC and Passports. The table below summarizes the Registrars who are

| UID Registrar | Primary Access ¹ | Additional Access ² | Potential Overlap | Effective Enrolment |
|----------------------|-----------------------------|--------------------------------|-------------------|---------------------|
| | Crore Residents | | | |
| LPG (Oil PSU) | 8.4 ³ | 16.8 ⁴ | 20% | 20.2 |
| LIC (Life Insurance) | 13.5 | 13.5 | 50% | 13.5 |
| PAN Cards | 4.0 | - | 75% | 1.0 |
| Passports | 6.0 | - | 80% | 1.2 |
| Urban Enrolment | | | | 35.9 |
| Lic (Life Insurance) | 3.5 | 3.5 | 90% | 0.7 |
| NREGA | 10.0 | 20.0 | 10% | 27.0 |
| BPL Ration Cards | 7.0 | 21.0 | 60% | 11.2 |
| State BPL/APL | 15.0 | 45.0 | 50% | 30.0 |
| Old Age Pensioners | 1.5 | 1.0 | 70% | 0.8 |
| Women/Child Welfare | 1.0 | 2.0 | 70% | 0.9 |
| Social Welfare | 1.0 | 2.0 | 70% | 0.9 |
| RSBY | 0.5 | 1.0 | 70% | 0.5 |
| Rural Enrolment | | | | 72.0 |
| Total Enrolment | | | | 107.9 |

In addition to these enrollers, the UIDAI will also partner with the Registrar General of India (RGI) – who will prepare the National Population Register through the Census 2011 – to reach as many residents as possible and enrol them into the UID database. This may require incorporating some additional procedures into the RGI data collection mechanism, in order to make it UID-ready.

3.3 A focused effort to enrol the poor and hard to reach groups

While the UIDAI intends to target Registrars that have large networks among the poor and rural communities in India, it will also emphasize multiple approaches to reach specific, frequently marginalized groups.

¹These are residents who are part of the Registrar's customer / subsidiary beneficiary database and can be mandated to provide their UID

²The residents under additional access are family members who can be easily covered while enrolling the primary residents. These can be all family members in the case of LPG connections and the nominees in case of LIC Policies,

³The total number of gas connections is 10.51 crores, and this estimates that there are 20% ineligible connections

⁴Assuming there are an average of three members in each family having a gas connection from an Oil PSU

Urban Poor

The urban poor are among the most ignored and disadvantaged people in India. The main challenges in enrolment here exist because this group consists mainly of migrant workers with temporary or seasonal jobs. The following may be ways to get them enrolled into the UID system.

Co-resident enrolment: Many of India's urban poor work as drivers, maids, or as workers associated with a family or a business. One approach to reach them could be for the head of the family or business to enable these members (who are co-residents/co-workers) to get enrolled into the UID with the same address proof the business or family uses. There can be a host of financial incentives offered to enrol such co-residents.

Financial institutions: The urban poor often borrow from micro-finance institutions and other sources and these could serve as enrolment points for them. There are established chit funds that can also act as enrolment points for the UID to improve coverage.

NGOs and Non-profits: There are several established non-profits working in urban slums in education, healthcare and social empowerment. They can be used to educate the poor on the benefits of the UID, for actual enrolment and to help endorse identity for people who lack documentation.

Children

India is a young country with over 400 million residents below the age of 18. While family-based government schemes will as Registrars, help enrol children, this population may need to be specifically targeted.

ICDS: ICDS is one of the world's largest integrated early childhood programs, with over 40,000 centers nationwide. The program covers over 5 million expectant and nursing mothers and 25 million children under the age of six. These centers can be information or enrolment points for non-school going children.

School admission: It may be mandated that at the time of joining school (first standard) it is necessary for children to have a UID or to enrol for one. This way the child can be tracked for progress and targeted for direct benefits.

The SSA program could also help enrol children in the 6-14 age group into the UID, which would also enable better child tracking and improvements in the mid-day meal schemes.

For children, the advantages from the UID would be significant. Child-related programs in India have relied on often inaccurate, aggregate data at school/cluster/block levels, making these programs ineffective. The concept of Universal Child Tracking – the ability to track every child and ensure their all round development – is gaining ground. An accurate database of children with UIDs would be immensely beneficial to programs within the Women and Child welfare as well as the Education departments, which track development in anganwadis and progress of children in government schools, and work to eliminate child labor.

Women

Apart from enrollers that are family-based government services in both urban and rural India such as PDS, RSBY etc, there needs to be a strategy to cover women outside this net:

Financial institutions: Robust collectives of women exist within micro-finance institutions and self-help groups across the country. These would be important enrolment points for women.

Organizations like Mahila Samakhyas in the 9 states of Karnataka, Kerala, Andhra Pradesh, Gujarat, Uttar Pradesh, Uttar Khand, Assam and Jharkhand. They work in several thousand villages to help women and can act as touch points for education or enrolment of women.

The National Commission for Women: This is the apex national level organization of India for protecting and promoting the interests of women. They have a massive outreach program that can reach out to disadvantaged women and get them to enrol. The UID can subsequently be used as a unique handle for a variety of services to be rendered to these women.

Differently-abled people

It is estimated that India has over 60 million differently-abled people, and identity for this population is a massive challenge. The Disability Act of 1995 mandates a certain percentage of employment for the differently-abled, but without the clear identification of such individuals, it is difficult to enforce the law. There is an obvious incentive for organizations like National Center for Promotion of Employment for Disabled People (NCPEDP) to promote the UID, and enable residents with disability to register for a range of benefits. The NGOs and rights groups associated with NCPEDP would also be good mechanisms to reach out to this section of the population.

Tribals

India has a significant tribal population of approximately 90 million tribals, mostly concentrated along a few states. The Government has many programs for the 697 notified tribes, which can be used for enrolment and information dissemination. In addition, NGOs and governments in states with high tribal populations can be Registrars for tribal groups.

The above mentioned approaches are merely indicative of the strategy that the UIDAI will follow to reach marginalized groups. In addition, the UIDAI will reach out to other marginalized groups such as homeless people, individuals in shelter homes, remand homes, asylums, etc.

Civil Society Outreach strategy

3.4 Enrolment costs

Enrolment costs can be thought of in two ways. One will be the cost to the enrolling agencies/Registrars for carrying out the enrolment process. The other costs will be to the residents to come to the enrolment stations. Poor may have to forego their wages for a day and also spend some travel costs to travel to the enrolment stations. The enrolment strategy will explore the

possibility of various mechanisms for funding the enrolment costs. The Registrars have the option here of charging for the cards they issue residents to offset enrolment costs. The UIDAI may issue guidelines around such pricing.

3.5 Ensuring clean enrolment data from Registrars

The UIDAI will periodically carry out a process audit of the information that comes in from the Registrars, to ensure data quality and that agencies are following guidelines recommended by the UIDAI. The audit would be on a random sample of residents, carried out either directly by the Authority or through appointed agencies. The audit might focus on:

Verification against scanned documents – The data contained in the resident records will be verified against the scanned documents.

Physical document verification – The physical documents that are held by the Registrar will be validated against the electronic copies.

Periodic process audits– Periodic audits will be carried out to at the enrolment sites, of the processes and software.

3.6 Updating UID details

Updating information with the UIDAI

The UID number is a lifetime number, but the biometric information contained in the central database will have to be regularly updated. Children may have to update their biometric information every five years, while adults update their information every ten years.

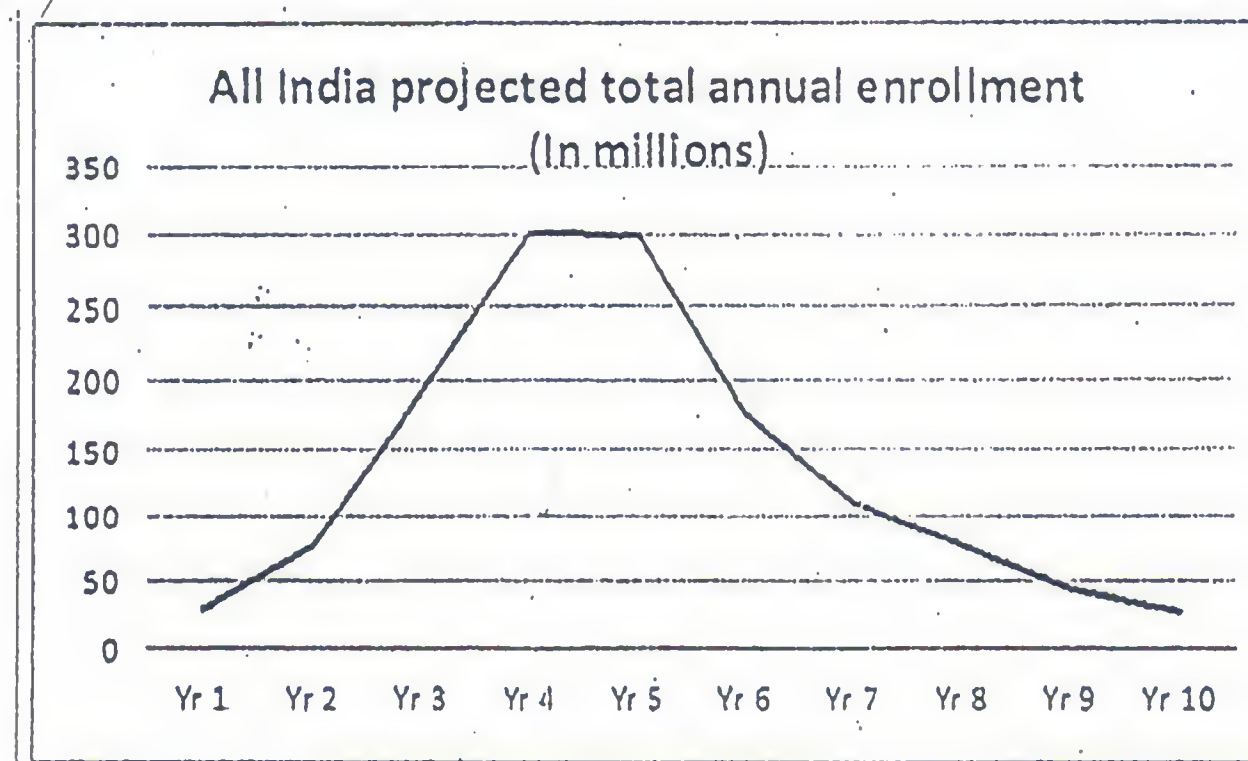
From time to time, the demographic information that the CIDR holds on the resident may also become outdated. Fields that are susceptible to change could be the 'present address' field, as well as the resident's name (after marriage). There might also be an error in the fields that occurred during enrolment into the UID.

If a service provider authenticating or enrolling a resident finds, through its KYR process that the information provided by the resident (address, name, etc.) does not match with the UID record, or that the biometrics need to be renewed, it can ask the resident to update their information in the UID database. The service provider may make the update a condition for the resident to receive the service/benefit.

Enrolling agencies and Registrars can serve as points where the resident can update their UID fields. The resident will have to submit their new information at these updation points with the required documentary evidence. This may also include a biometric authentication prior to processing the request.



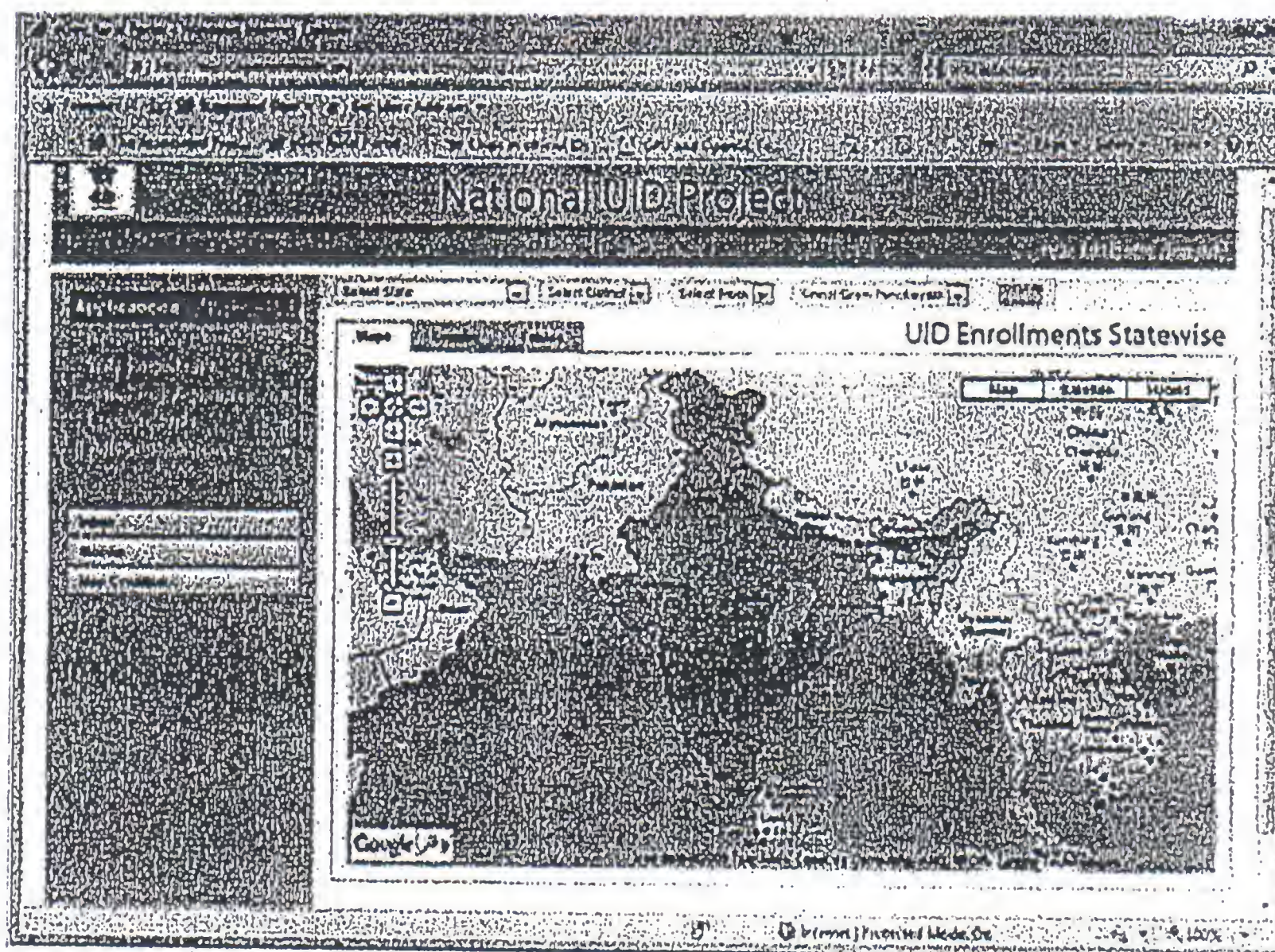
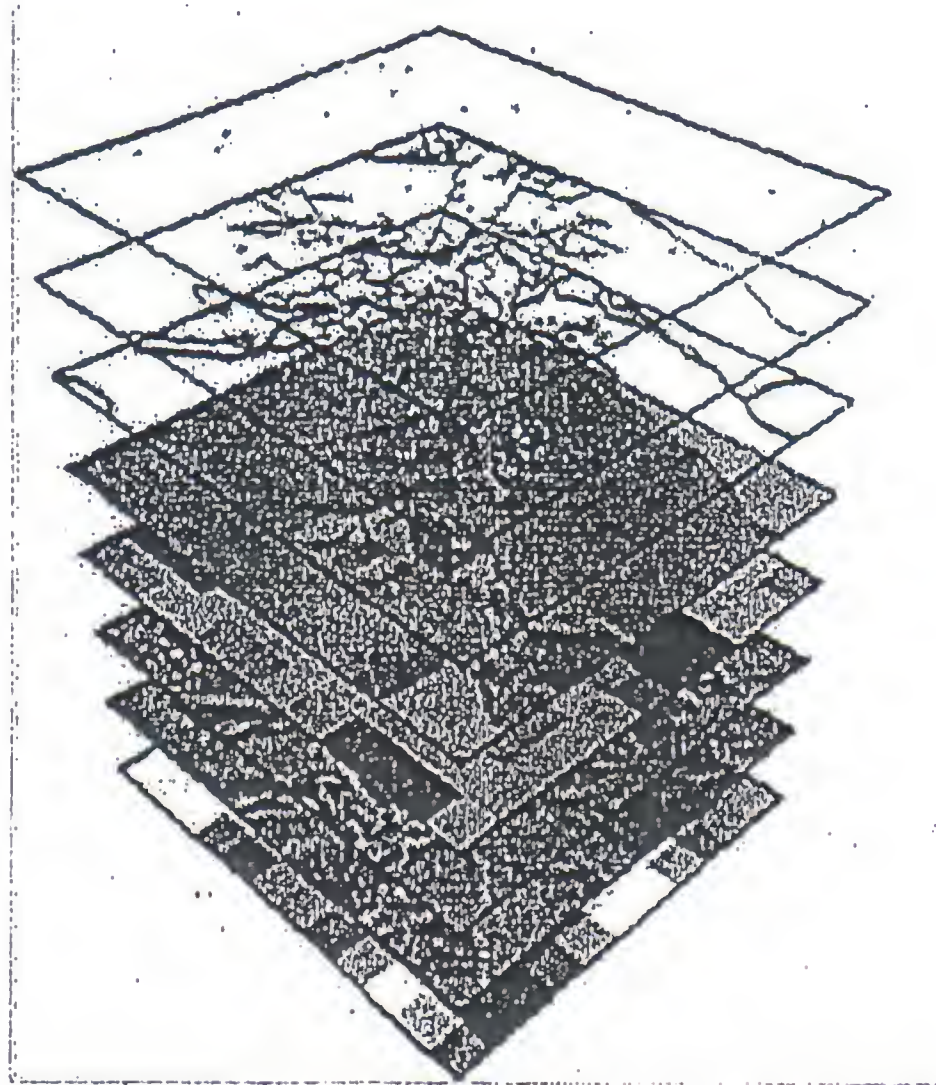
• 142



24
89

3.8 Tracking enrolments across the country

The UIDAI will employ a GIS internet-based visual reporting system to track enrolment trends and patterns across India; as the project is rolled out across various Registrars and states.



The GIS system will show all UID enrolments by state, as well as by Registrar. The system will also be able to drill down within states and into districts.

3.9 Reaching a sustainable, steady-state in enrolment

A challenge for full enrolment is registering the approximately 60,000 babies that are born in the country every day. Over the next several years, the UIDAI expects to enrol close to the entire Indian population. Once that goal is achieved, enrolment will reach a steady state, where only births (and deaths) as well as immigrants need to be recorded.

There are however, some challenges in registering new births. First, since their biometrics is not stable, they have to be re-scanned at a later age. Second, names are often not given in India at the time of birth registration.

The UID in the birth certificate

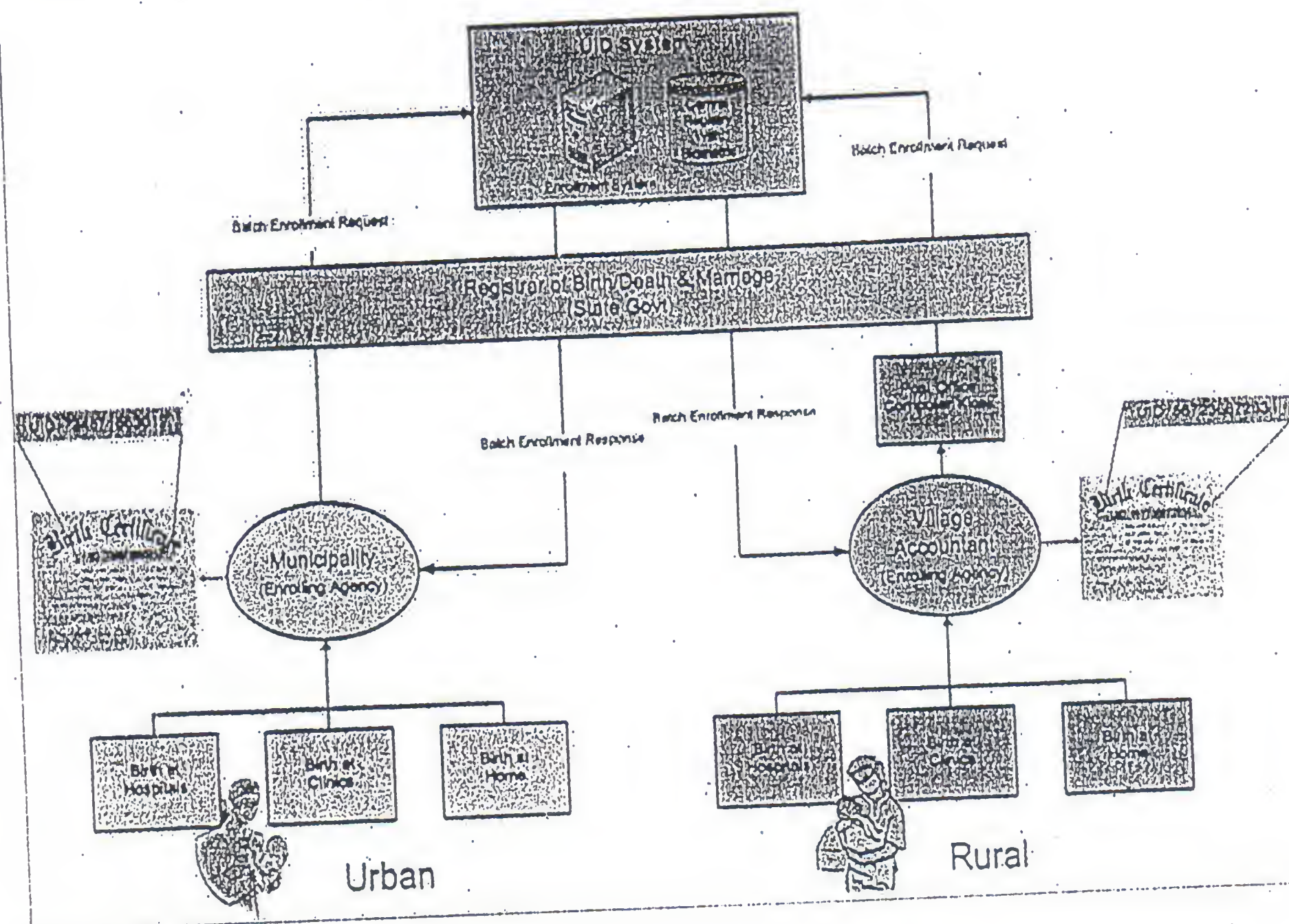
One way to ensure that the UID number is used by all government and private agencies is by inserting it into the birth certificate of the infant. Since the birth certificate is the original identity document, it is likely that this number will then persist as the key identifier through the individual's various life events, such as joining school, immunizations, voting etc.

Since the name is a mandatory field in the UID database, it is essential that the child be given a name before applying for the UID number. This would ensure that the UID can also be allotted at birth.

In the case of urban births, the municipality will be the enrolling authority and the UID Registrar can be the 'Registrar of Births, Deaths and Marriage' at the state level.

In rural areas, births take place at district or block level hospitals, in health care centers and at homes in the village. The village accountant is the Registrar of rural births, and he/she also issues the birth certificate and updates the information through an enrolling agency.





Biometrics and infants

The recording of unique individual biometrics in the UID database is a challenging one for infant records. The solution to this is to record the UID and biometric of the parents in the child's record.

The child's biometrics need to be taken at around 5 years of age, and updated in the UID system every 5 years until the age of 18. This will be enforced by an expiry date attached to the UID number, which will become invalid after that date. Until the time the biometric of the child stabilizes, any one of the parents/guardian will need to provide their biometric information for authentication.

Recording deaths in the UID system

It is also necessary to record deaths in the country, and the birth and death registration act provides for such registration. The same institutions that record births can be in charge of updating deaths in the UID system. The UID system will not remove a record upon the person's death; it will simply mark it as 'deceased' and hence will render it inactive for the purposes of authentication.

4

Ensuring strong authentication and what it means for the UIDAI

The real test of reliability for the UID system will be during identity authentication. Confirming 'you are who you say you are' remains the primary, often elusive goal of all identity systems.

The UIDAI approach – which will be online authentication, with biometric check – creates a very strong authentication system, and gives the UIDAI significant ability to confirm an individual's identity. The UIDAI will support the Registrars in building the infrastructure and systems necessary to authenticate residents in different parts of the country. This will be especially critical for Registrars working in rural areas and among the poor.

4.1 Enabling UID adoption for authentication

The speed of UID adoption in India depends on whether the number can help in eliminating poverty and marginalization, and in enabling greater transparency and efficiency in service delivery. If it succeeds in these goals, the number will become indispensable for residents in accessing services.

While the UID can provide the strongest form of pre-verification and identity authentication in the country, it cannot ensure that targeted benefit programs reach intended beneficiaries. The poor impact of the UID, consequently, will not gain traction unless there is a mechanism to link the UID process with actual service delivery.

A clear adoption process can overcome this gap by helping introduce the UID method of authentication at every point of service delivery. To ensure this, the UIDAI will not only work with Registrars who do enrolment, but also with non-enrolling, service delivery agencies. Such agencies involved in the delivery of services and benefits will be encouraged to partner with the UIDAI for authentication. Once they authenticate a resident's identity against the UID database every time they carry out a service transaction, they will be able to deliver services far more effectively.

In order to accommodate this authentication, agencies may need to re-engineer their business processes to be UID-enabled. The most basic requirement for change will be in incorporating the UID method of authentication into their systems. Agencies will have to adhere to norms and procedures specified by the UIDAI for fingerprint capture and verification, and introduce a robust biometric authentication process at every point of sale.

There is tremendous value to be gained from widespread adoption of the UID for authentication, especially for residents. While enrolment in the UID database will ensure that residents are not denied access to fundamental services and rights because they cannot present positive proof of identity, adoption in authentication could go one step further, and ensure that residents

consistently receive these services. This can include a wide range of benefits such as education, health coverage, old-age pensions and subsidized food grains, thereby fulfilling the UIDAI's pro-poor agenda.

The UIDAI is only in the identity domain. The responsibility of tracking beneficiaries and the governance of service delivery will continue to remain with the respective agencies – the job of tracking distribution of food grains among BPL families for example, will remain with the state PDS department. The adoption of the UID will only ensure that the uniqueness and singularity of each resident is established and authenticated, thereby promoting equitable access to social services.

The adoption of the UID during authentication will also have a direct correlation with subsequent enrolment. Greater enrolment comes from the value a resident derives from the UID, which in turn depends on the rate of adoption. There is a positive cycle here, created from the relationship between adoption and enrolment – the greater the adoption, the faster the enrolment and vice versa. The twin approaches of enrolment and adoption will result in greater influence and traction for the UID among residents in the country, and establish the UIDAI as the only genuine identity authenticator in India.

4.2 Types of authentication

There are multiple forms of authentication that the UID authority can offer. Certain types of authentication would have low to medium assurance if there is the possibility that the card is forged. Here we summarize the main forms of authentication, depending on the situation and equipment available.

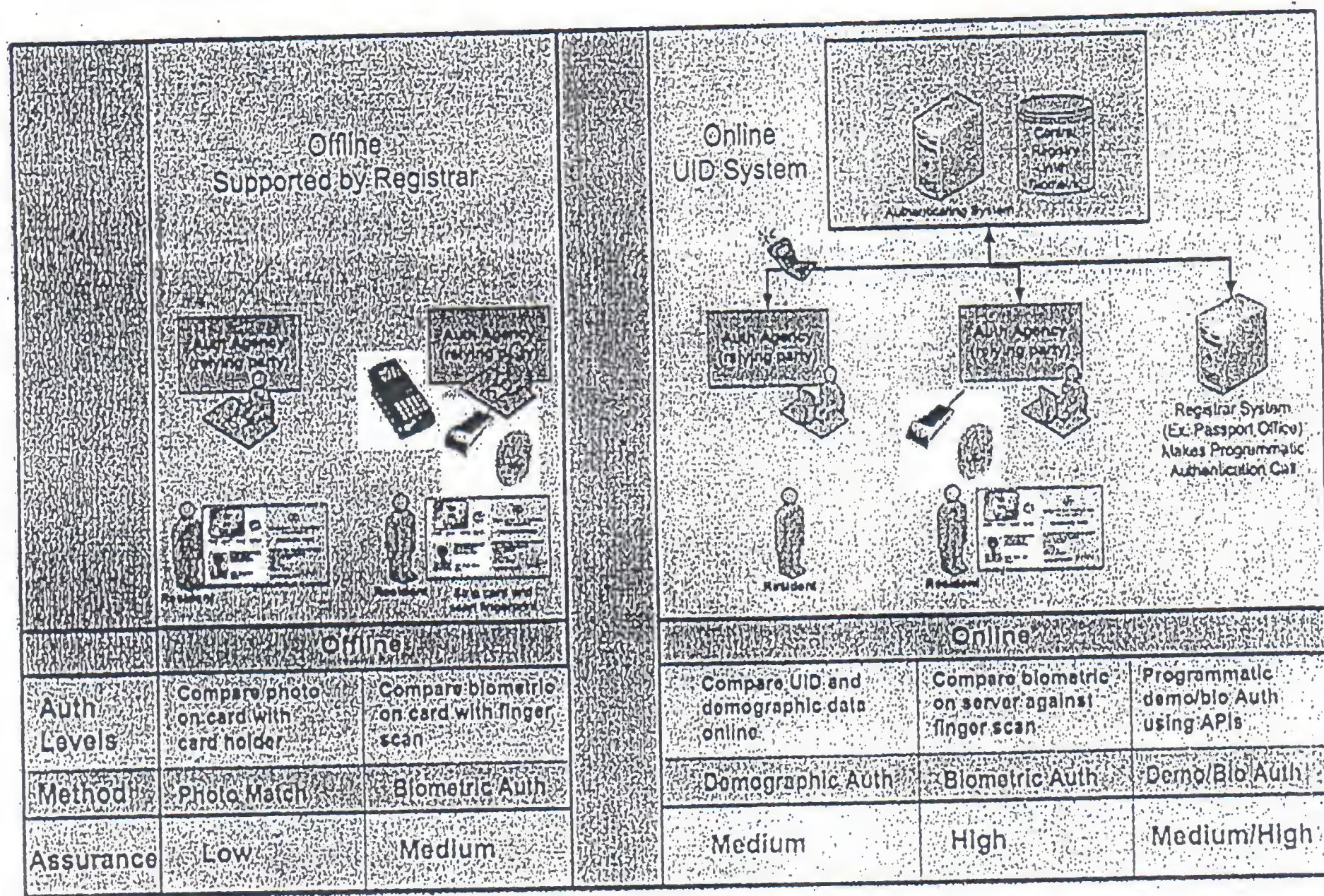
Online authentication is supported by the UID system. This can include

- Online demographic authentication where the authenticating agency compares the UID number and demographic information of the UID holder to the information stored in the UID database. The assurance level here is medium.
- Online biometric authentication where the biometrics of the UID holder, his UID and key demographic details are compared to the details in the CIDR. The assurance level in this case is high.
- Online demographic/biometric authentication with API where the Registrar's backend system makes a programmatic call to the authentication APIs exposed by the UID system to perform authentication. The assurance level here may be medium-high depending on whether the check used demographic or biometric inputs.

Offline authentication may be supported by the Registrar, and does not use the authenticating service provided by the UIDAI. This may come in two forms:

- Photo match authentication where the photo on the card is compared with the cardholder. This is the most basic form of authentication. The assurance level here is low.

Offline biometric authentication compares the scanned fingerprint of the cardholder to the biometric stored on the Registrar-issued card. The assurance level here is medium.



4.3 Authentication and the UIDAI revenue model

The ability of the UIDAI to offer agencies across the country strong, reliable authentication is the key to its sustainability. The UIDAI will offer resident authentication services for a fee to governments and private sector firms.

The agencies which request a resident authentication service will have to be registered with the UIDAI and follow strict guidelines in using the service as well as in managing resident information.

Basic Identity confirmation

Basic identity confirmation from the UIDAI would be free. In this transaction, the authenticator will provide the UID number, name and one other parameter such as date of birth of the person, and the central database will confirm the identity as a 'Yes' or 'No' response.

This type of transaction will be carried out in large numbers and will need quick response times.

Chargeable authentication services can be of two types:

Address verification

For security purposes, government agencies as well as private sector firms require address proof

from Indian residents before providing them with benefits and services. However, agencies often complain of the difficulty of address verification "you try to verify an address in India, and you enter a labyrinth". The service provider usually verifies address through a physical visit, as well as an enquiry to confirm the other information provided. This process is expensive and costs between Rs. 100 and Rs. 500 per verification.

The address authentication service the UIDAI will offer these entities would consequently be a valuable one. In the proposed transaction with the UID Authority, the agency will submit the UID, name and address of the resident to the CIDR, which will confirm the address. As a result, the agency will not have to do physical address verification.

Biometrics confirmation

Services such as issuing a credit card or granting a loan need the confirmation of the resident's identity. This process for the resident involves the submission of photographs and other documentation confirming their identity. In the proposed transaction with the UID Authority, the agency can send the scanned photograph or fingerprint (based on the security level required) together with other demographic details to confirm the identity of the person.

Revenue projections from authentication services

The following revenue model for the UIDAI is an illustrative one. It has been designed while keeping in mind the value the agency requesting authentication would derive from the service. The table below summarizes the kind of transaction, potential user agencies and the proposed transaction fee. Government agencies could be provided these services from the UIDAI at a subsidized rate.

| Sl. | Transaction Type | Transaction Fee | Potential User Agencies |
|-----|-------------------------|-----------------|------------------------------------|
| 1 | Basic ID Confirmation | Free | Airlines during passenger check-in |
| 2 | Address Verification | Rs. 5 | Banks for account opening |
| 3 | Biometrics Confirmation | Rs. 10 | Credit cards issue process |

The authentication service from the UIDAI can begin after the initial bulk on-boarding of Registrars. The revenue estimates for the UIDAI below are based on the current expenditure of various agencies on KYR processes, which would be replaced by the Authority's authentication services. It also takes into account expected growth in demand for mobile connections, bank accounts, etc.

| UID Revenue Projection (Steady State Estimates) | Transaction Type | |
|--|------------------|------------|
| | Address | Biometrics |
| New Mobile Connections | 19.59 | - |
| PAN Cards | - | 1.20 |
| Gas Connections by PSU | - | 1.50 |
| Passports | 0.06 | - |
| LIC New Policies | - | 10.16 |
| Credit Cards | 0.70 | - |
| Bank Accounts | 11.55 | - |
| Airline Check-in | - | - |
| Projected Total Transactions | 31.91 | 12.86 |
| Proposed Transaction Rate | 5 | 10 |
| Transaction Revenue | 159.55 | 128.60 |
| Estimated total annual revenue at steady state (Rs. Crores) | | 288.15 |

5

Legal Framework

The Constitution of India, through the Directive Principles of State Policy⁵ mandates that the state shall strive to minimize inequalities of income and endeavor to eliminate inequalities in status amongst individuals. The objective of the UIDAI is to solve the key problem of identity that individuals face and enable better and efficient delivery of services to the poor and marginalized so as to eliminate inequalities of income and status. It is therefore, imperative to have a proper legal structure in place to ensure the smooth functioning of the UIDAI. This section provides an overview of the legal and policy framework.

The Unique Identification Authority of India (UIDAI) will be set up as a statutory body by an Act of Parliament. The UIDAI will be authorized:

- o To collect the following identity information from any person voluntarily seeking a unique identity number:
 - Name
 - Date of Birth
 - Gender
 - Father's name and UID number
 - Mother's name and UID number
 - Address
 - All ten finger prints, photograph and both iris scans

The law will contain a prescription against collecting any other information than the information permitted, with specific prohibitions against collection of information regarding religion, race, ethnicity, caste and other similar matters, and for the facilitation of analysis of the data for anyone or to engage in profiling or any similar activity.

- o To issue a unique identity number to the person who has provided the necessary information and fulfilled the requirements as laid down in rules prescribed by the UIDAI.

Art. 38 ⁵ (1) The State shall strive to promote the welfare of the people by securing and protecting as effectively as it may a social order in which justice, social, economic and political, shall inform all the institutions of the national life.

(2) The State shall, in particular, strive to minimise the inequalities in income, and endeavour to eliminate inequalities in status, facilities and opportunities, not only amongst individuals but also amongst groups of people residing in different areas or engaged in different vocations.

- o To verify the identity of any person at the time of the provision of information, the issuance of a unique identity number or at any other time per the UIDAI database or other possible means, as laid down in rules prescribed by the UIDAI.
- o To permit the UIDAI to set up or facilitate the infrastructure by which third parties can authenticate the identity of persons who have provided information to the UIDAI and the circumstances and conditions they can seek such verification. The information on the database will be used only to authenticate identity.
- o To establish or appoint a Central ID Data Repository (CIDR) for the purposes of collecting, managing and securing the database and to outsource any such functions.
- o To permit the appointment of Registrars in accordance with criteria laid down by the UIDAI to enrol people that seek unique identity numbers directly or indirectly through enrolling agencies.
- o To allow for the appointment of other service providers in accordance with criteria laid down by the UIDAI, as the UIDAI may deem fit to further its objectives and to ensure efficiency.
- o To call for information and records, conduct inspections, inquiries and audit of the CIDR, Registrars, enrolling agencies and service providers..
- o To enter into all necessary contracts and arrangements in order to fulfill the objectives of the UIDAI.
- o To set up mechanisms for grievance redressal for the public
- o To set up a monitoring framework to improve implementation, create safeguards as required and study the impact of the UID
- o To hire the necessary technical and professional personnel necessary for executing the mandate and fulfill the objectives of the UIDAI.

The law will also contain

- o Penal provisions against persons employed by, or associated directly or indirectly with, the CIDR, Registrars, enrolling agencies and other service providers for failing to comply with the directions issued under the Act
- o Penal provisions against persons employed by, or associated directly or indirectly with the UIDAI, CIDR, Registrars, enrolling agencies and other service providers for breach of certain key sections of the legislation – including the specific prohibitions on profiling, the disclosure of information and maintenance of confidentiality etc.
- o Penal provision for persons who intentionally or fraudulently provide wrong information, attempt to obtain a second unique identity number, steal the identity of any living or dead

34
99

person, etc. In this context, there will be no liability on the part of the UIDAI or persons employed by, or associated directly or indirectly with the UIDAI, CIDR, Registrars, enrolling agencies and other service providers for providing a unique identity number to a person who intentionally or fraudulently obtains such number.

Protecting privacy and confidentiality

The information that the UIDAI is seeking is already available with several agencies (public and private) in the country, the additional information being sought by the UIDAI are the finger prints and iris scans. However, the UIDAI recognizes that the right of privacy must be protected, and that people are sensitive to the idea of giving out their personal information, particularly the idea of information being stored in a central database to be used for authentication. UIDAI will protect the right to privacy of the person seeking the unique identity number. The information on the database will be used only to authenticate identity. Necessary provisions would be in place to address the issues of privacy and confidentiality.

Offences under the UIDAI Act

The UID database will be susceptible to attacks and leaks at various levels. The UIDAI must have enough teeth to be able to address and deal with these issues effectively. It will be an offence under the UIDAI Act to engage in the following activities:

- Unauthorized disclosure of information by anyone in the UIDAI, Registrar or the Enrolling agency
- Disclosure of information violating the protocols set in place by the UIDAI
- Sharing any of the data on the database with anyone.
- Engaging in or facilitating analysis of the data for anyone.
- Engaging in or facilitating profiling of any nature for anyone or providing information for profiling of any nature for anyone.
- All offences under the Information Technology Act shall be deemed to be offences under the UIDAI if directed against the UIDAI or its database.

6

Data Security and Fraud

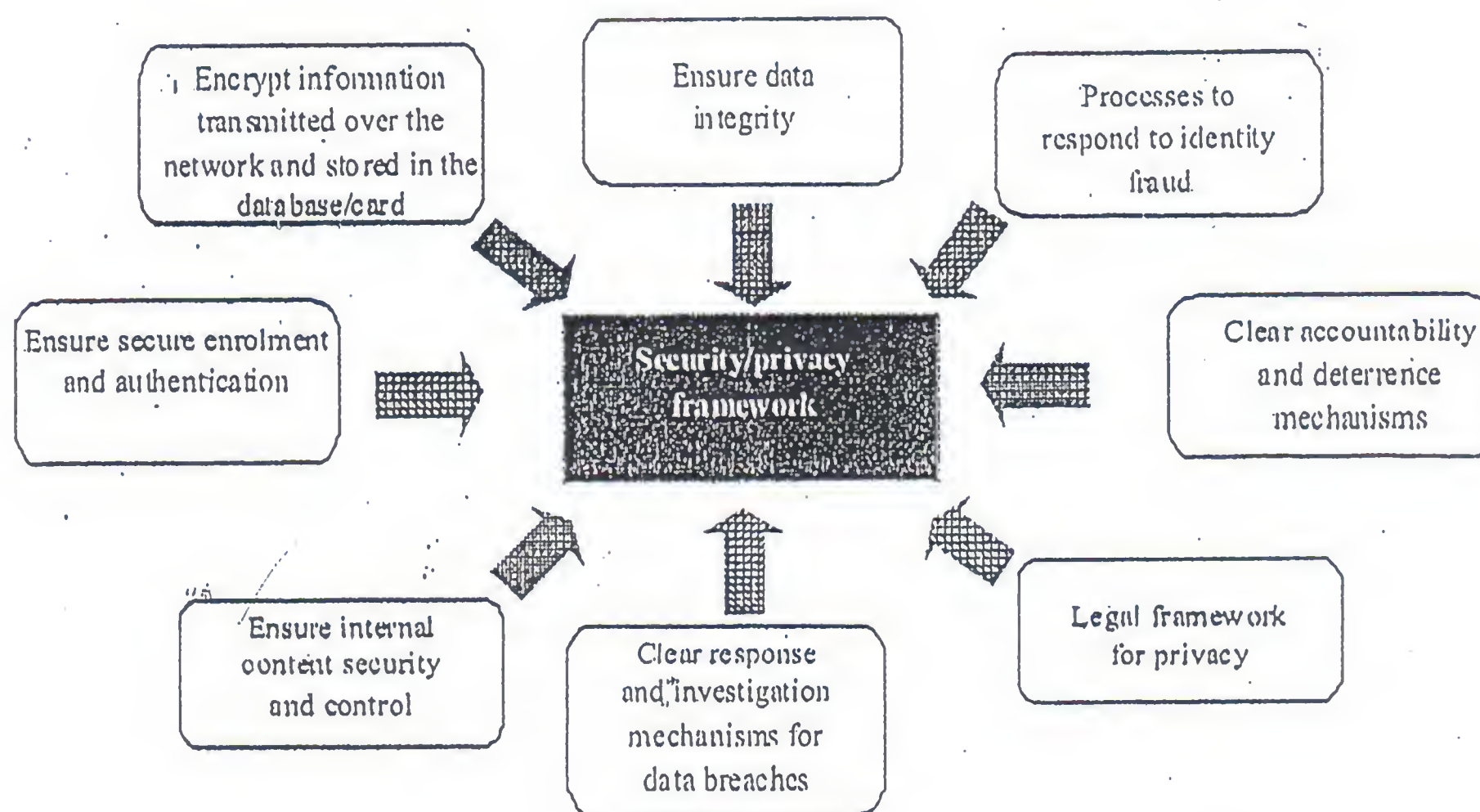
6.1 Protecting personal information of residents

Even as the UIDAI stores resident information and confirms identity to authenticating agencies, it will have to ensure the security and privacy of such information.

By linking an individual's personal, identifying information to a UID, the UIDAI will be creating a transaction identity for each resident that is both verified and reliable. This means that the resident's identity will possess value, and enable the transfer of money and resources.

The UIDAI envisions storing basic personal information, as well as certain biometrics. However, limiting its scope to this, and not linking this information to financial/other details does not make the resident records in the database non-sensitive. Biometric information for example, is often linked to banking, social security and passport records. Basic personal information such as date of birth is used to verify owners of credit card/bank accounts and online accounts. Such information will therefore, have to be protected. Loss of this information risks the resident's financial and other assets, as well as reputation, when the resident is a victim of identity theft.

In the federated system that the UIDAI envisions, we must consequently have processes in place to ensure a fair level of data security.



6.2 Fraud scenarios

The Authority will concern itself only with identity fraud, which is distinct from document fraud. Document fraud, the use of counterfeited/misleading documents to enter incorrect personal information, will be the responsibility of the Registrar enrolling the resident. The Authority will have clear response mechanisms in place for identity fraud, where an individual deliberately impersonates someone else, either real or fictitious.

Since the CIDR will store the biometric of residents, identity fraud will be easier to control. The only form of fraud that may go undetected in the UID system is if a person registers his/her details and biometrics under an entirely different name, with forged supporting documents. However, the person will have to exist under this name across systems, in the lifetime of his/her interaction with the government, private agencies and service providers. Such instances are therefore, likely to be rare.

Some of the potential fraud scenarios are:

| Scenario | Response |
|--|---|
| Person applies for a UID number and presents wrong information under their name. | The verification process returns application to the applicant and presents the reasons for not issuing number. |
| Person applies to get a second card in another name. | Application returned, with reason provided. If person's name was fraudulent the first time, he has the option of applying to change his demographic fields. If this fraud is attempted again, person is added to watch list/ legal action. |
| Person appears as himself, and applies for a second UID number. | Application returned, with reason provided. If attempted more than three times person added to watch list. |
| Person appears as another existing person, registering the second person's information under his fingerprint. Impersonation of a deceased individual, with fake supporting documents. | The victim can report identity theft to the UIDAI's grievance office. The UIDAI will undertake an investigation, and take appropriate action if theft is confirmed. If the applicant passes the verification process, then he may be able to take on the stolen identity. However, he will not be able to change his demographic fields over his lifetime without due process. |
| De-duplication works incorrectly and returns false positive for a new UID applicant. | Person can request check against face biometrics as well as re-verification by Registrar. |

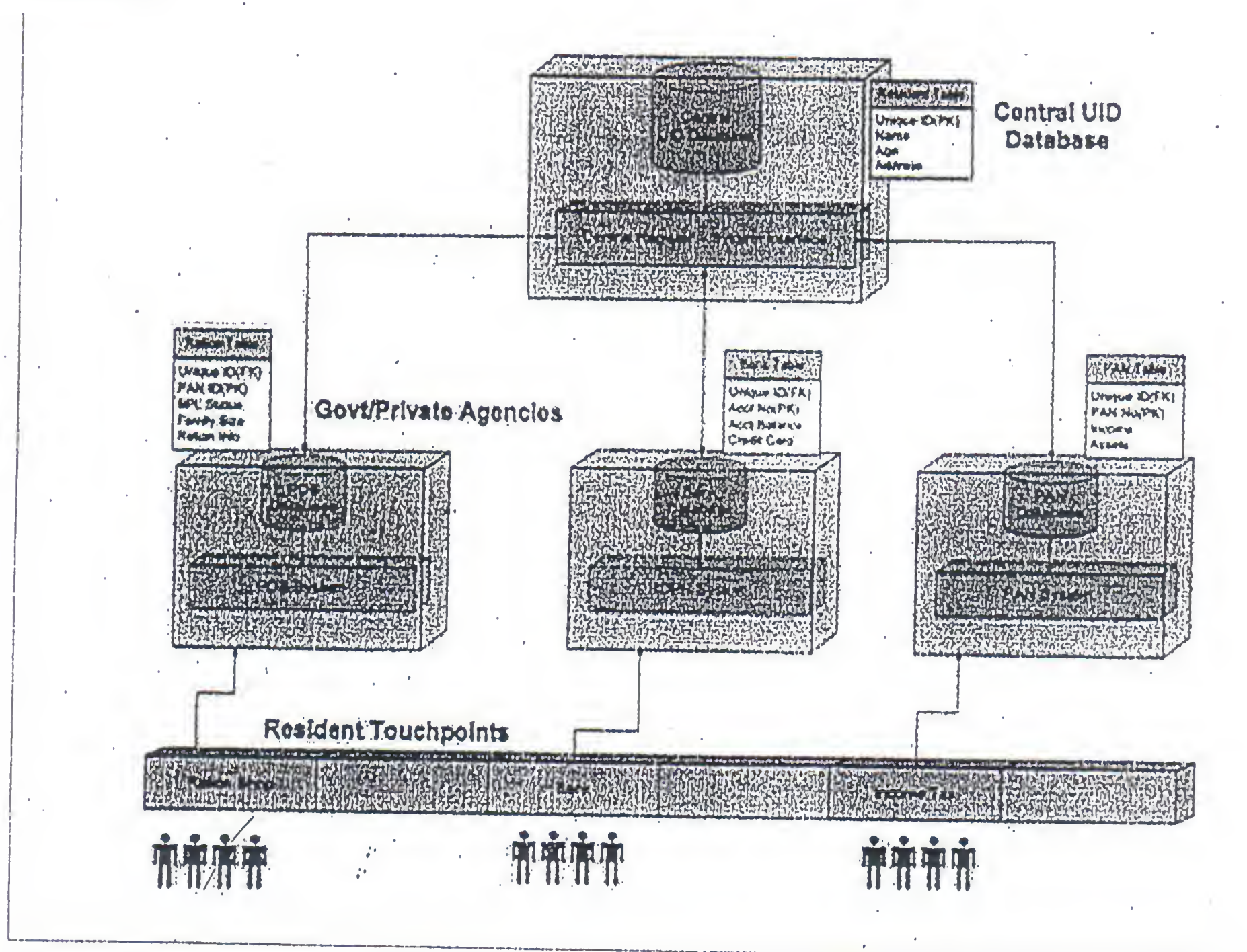
7

Technology architecture of the UIDAI

The technical architecture of the UIDAI is at this point, based on high-level assumptions. The architecture has been structured to ensure clear data verification, authentication and de-duplication, while ensuring a high level of privacy and information security.

7.1 System architecture

The Central ID Data Repository will be the central database of all residents, containing the minimal set of fields sufficient to confirm identity. The federated set of databases belonging to the Registrars may contain additional information about the resident, and can use the resident's UID as the key.



The key technology components of the UID system are:

- **The UID Server**, which provides the enrolment and the authentication service. These services will be available over the network for the various Registrars and their authenticating agencies to use. The backend servers need to be architected for the high

demands of the 1:N biometric de-duplication as well as the large peak loads from authentication requests.

- **The Biometric sub-system** is central to the UID system for enrolling as well as authenticating residents. It is likely that a multi-modal biometric solution will be used to achieve a high level of assurance. The 1:N de-duplication envisioned will be by far the most computing-intensive operation of the UID system. Innovative techniques of hashing, indexing, distributed processing, and in-memory databases using multiple-biometric-modes need to be employed to get acceptable performance.
- **The Enrolment client** application will capture and validate demographic and biometric data. This client needs to work in an offline mode in the village setting when there is no internet connectivity, and upload batch files to the server for processing. Alternatively the batch files can be physically transported to the CIDR for uploading. The client application will be deployed on a standard enrolment workstation.
- **The Network** is a critical aspect of the system, since all UID enrolment and authentication services will be available online. UID services could work over secure WAN networks, the vanilla internet or over mobile SMS channels. It could also potentially work over existing networks such as credit-card POS (point-of-service) devices.
- **The Security design** secures all the above components from logical/physical attack. This includes.
 - Server Security – firewall, intrusion prevention and detection systems (IPS, IDS)
 - Network, Client Security – Encryption, PKI etc
- **The Administration system** will help administer the UIDAI's operations. This includes
 - Account setup – creation/modification of Registrar, enrolling and authenticating agency accounts.
 - Role-based access control – Assign rights over UID resources based on role.
 - Audit trailing – track every access to the UID system.
 - Fraud detection – detect identity theft and cyber crimes using audit trails
 - Reporting and Analytics – Visual decision support tools – GIS, Charting etc.

8

Project Execution

One of the unique challenges in executing the UID project is its scale. Due to the size of India's population, the UIDAI is undertaking what is perhaps the largest governance-related exercise in the world. We must ensure that all aspects of the project – enrolment, de-duplication, and authentication – function effectively even as the number of records approaches a billion.

8.1 Addressing challenges of scale

The UIDAI can expect its enrolment run-rate to have a peak load of one million enrolments per day in the very first year of operation. Every sub-system and component of the UID system will need to scale quickly and significantly. This will include:

- 1) The ability to onboard Registrars from different sectors and handle their constituencies of residents.
- 2) The legal framework of contracts needs to support the variety and spread of stakeholders as their numbers grow exponentially across the country.
- 3) The biometric de-duplication algorithm needs to scale towards checking a fingerprint against every one of 1.2 billion people to ensure uniqueness.
- 4) The authenticating service, which may be used by tens of thousands of points across the country, needs to scale to handle hundreds of thousands of transactions per second.

9

Project Risk

The UID project does face certain risks in its implementation, which have to be addressed through its architecture and the design of its incentives. Some of these risks include:

- 1) **Adoption risks:** There will have to be sufficient, early demand from residents for the UID number. Without critical mass among key demographic groups (the rural and the poor) the number will not be successful in the long term. To ensure this, the UIDAI will have to model de-duplication and authentication to be both effective and viable for participating agencies and service providers.
- 2) **Political risks:** The UID project will require support from state governments across India. The project will also require sufficient support from individual government departments, especially in linking public services to the UID, and from service providers joining as Registrars.
- 3) **Enrolment risks:** The project will have to be carefully designed to address risks of low enrolment – such as creating sufficient touch points in rural areas, enabling and motivating Registrars, ensuring that documentary requirements don't derail enrolment in disadvantaged communities – as well as managing difficulties in address verification, name standards, lack of information on date of birth, and hard to record fingerprints.
- 4) **Risks of scale:** The project will have to handle records that approach one billion in number. This creates significant risks in biometric de-duplication as well as in administration, storage, and continued expansion of infrastructure.
- 5) **Technology risks:** Technology is a key part of the UID program, and this is the first time in the world that storage, authentication and de-duplication of biometrics are being attempted on this scale. The authority will have to address the risks carefully – by choosing the right technology in the architecture, biometrics, and data management tools; managing obsolescence and data quality; designing the transaction services model and innovating towards the best possible result.
- 6) **Privacy and security risks:** The UIDAI will have to ensure that resident data is not shared or compromised.
- 7) **Sustainability risks:** The economic model for the UIDAI will have to be designed to be sustainable in the long-term, and ensure that the project can adhere to the standards mandated by the Authority.

10

UID-enabled micro-payment architecture

This section discusses one of the potential applications of the UID – the use of the number in driving financial inclusion, and in enabling a micropayments solution that the poor can use to access financial services.

While the demand for financial inclusion has gained urgency over the last few years, initiatives in India to expand financial infrastructure date back several decades, since the building of rural cooperative credit banks in the 1950s, and the spread of bank networks in the 1970s and 1980s. These initiatives have paid off over the years — India's bank branches are well-networked, particularly across urban India.

But despite these efforts, access to finance has remained scarce in rural India, and for the poorest residents in the country. Today, the proportion of rural residents who lack access to bank accounts remains at 40%, and this rises to over three-fifths of the population in the east and north-east of India.

This exclusion is unfortunate. Economic opportunity is after all, intertwined with financial access. Such financial access is especially valuable for the poor — it offers a cushion to a group whose incomes are often volatile and small. It gives them opportunities to build savings, insure themselves against income shocks and make investments. Such savings and insurance protect the poor against potentially ruinous events — illness, loss of employment, droughts, and crop failures. However due to the lack of access to financial services, many of the Indian poor face difficulties in accumulating savings.

To mitigate the lack of financial access in India, the RBI has focused on improving the reach of financial services in new and innovative ways — through no-frills accounts, the liberalization of banking and ATM policies, and branchless banking with business correspondents² (BC), which enables local intermediaries such as self-help groups, post offices and kirana stores to provide banking services. These efforts have also included the promotion of core-banking solutions in regional rural banks; and the incorporation of the National Payment Corporation of India (NPCI) as an apex switch, for payments and settlements.

In recent years, ATM and core banking, as well as greater mobile connectivity have also become two powerful engines of financial access. Mobile phones in particular present an enormous opportunity in spreading financial services across India. These technologies have reduced the need for banks to be physically close to their customers, and banks have been consequently able to experiment with providing services through online as well as mobile banking. These options, in addition to ATMs, have made banking accessible and affordable for many urban non-poor residents across the country.

42
107

With the poor however, banks face a fundamental challenge that limits the success of these technologies and recent banking innovations. The lack of clear identity documentation for the poor creates substantial difficulties in establishing their identity to banks. This has limited the extent to which we can leverage online and mobile banking to reach these communities.

Besides challenges in access and identity, a third limitation has been the cost of providing banking services for the poor. The poor have unique preferences when it comes to withdrawing money and making deposits — they prefer to do large numbers of small transactions, in 'micropayments' of say, Rs.10 rather than Rs.100. Banks discourage such payments, as transaction costs under this model would be too high to bear. The Unique Identification number (UID), which identifies individuals uniquely on the basis of their demographic information and biometrics, gives individuals the means to clearly establish their identity to public and private agencies across the country. It also creates an opportunity to address the existing limitations in financial inclusion. The UID, once it's linked to a bank account, can help poor residents easily establish their identity to banking institutions. As a result, the UID enables banking institutions to bring together the infrastructure that now exists in order to build an accessible, low-cost micropayments model.

Since the UID enables remote authentication of identity, it empowers the poor in making electronic transactions in small, micro-amounts, remotely and at low-cost, through BC networks connected by mobile phones. The model would thus be accessible and affordable across the country. Such a UID-enabled micropayments approach can bring about universal financial access for the poor — they would be able to access their accounts on the move, wherever they are, through any mobile phone, from any BC or bank. The UID-enabled bank account can thus be a global address for residents, similar to an email id or a mobile phone number.

Over the last few years, we have seen critical reforms implemented towards creating a payments solution for the poor. The UID number helps integrate these reforms and leverage the technology already in place into an effective micropayments solution. This can bring low-cost access to financial services to everyone, a short distance from their homes.

10.1 Features of UID-enabled micropayments

UID KYR sufficient for KYC: Banks in India are required to follow customer identification procedures while opening new accounts, to reduce the risk of fraud and money laundering. The strong authentication that the UID offers, combined with its KYR standards, could remove the need for such individual KYC by banking institutions for basic, no-frills accounts. It will thus vastly reduce the documentation the poor are required to produce for a bank account, and significantly bring down KYC costs for banks.

Electronic transactions: The UID's authentication processes will allow banking institutions to verify poor residents both in person and remotely. Rural residents will be able to transact electronically with each other as well as with individuals and firms outside the village, reducing their dependence on cash.

Ubiquitous BC network and BC choice: The UID's clear authentication and verification processes will allow banking institutions to network with village-based BCs such as self-help groups, post offices and kirana stores. Customers will be able to withdraw money and make deposits at the local BC. Multiple BCs at the local level will also give customers a choice of BCs. This would make customers, particularly in villages, less vulnerable to local power structures, and lower the risk of being exploited by BCs.

A high-volume, low-cost revenue approach: The UID will mitigate the high customer acquisition costs, high transaction costs and fixed IT costs that we now face in bringing bank accounts to the poor.

No-frills accounts that can be provided and accessed at low cost through local BCs, with electronic cash transfers, would encourage large numbers of small transactions across these accounts, and make these accounts an important source of revenue for banks.

10.2 Benefits

For residents: The UID-enabled Bank Account (UEBA) will bring financial access and affordability to millions of residents who are presently excluded from formal financial systems. A UID-enabled bank account will also help residents make cheaper, faster electronic transactions and remittances in the form of micropayments. The solution will enable universal access to their account from any bank or BC, and through any mobile device, enabling residents to access payments on the move. Regular, affordable access to banking services would also give the poor a means of keeping their money safe — a convenience that has long been available to the middle class would now be accessible to the rural and urban poor.

For the government: Large-scale financial inclusion can pave the way for electronic benefit transfers (EBTs) for residents. Central and state governments will be able to eliminate the identity-related fraud that exists within its public programs with such transfers going into UID-enabled bank accounts. The bulk of the informal cash economy across rural India, and remittances between urban and rural India will also become part of the formal banking system, with traceable and accountable money flows. This will ensure compliance with Anti-Money Laundering laws and Financial Action Task Force standards. The government will gain these benefits without having to overhaul governance systems — the micropayments approach won't require governments to change decision-making processes across the central, state and local level.

For banking institutions: The use of the central payments switch to move cash electronically at the last mile will dramatically cut down on cash handling and transaction costs for banking institutions. The cost of customer acquisition would also be significantly reduced, as a resident with a UID would require no further identification to get a UID-enabled bank account.

A low-cost micropayment approach will make the large volume of micropayments, remittances and government transfers to UID-enabled bank accounts important sources of revenue for banking institutions. Through the BC network, banks would be able to access customers through

the large distribution channels in the country — including the mobile prepaid network, post office network and FMCG retailers. In addition, BCs would see increased revenues from larger numbers of micro-transactions.

10.3 Conclusion

Over the last decade, we have seen a transformation in financial access for residents across the country — the reforms that encouraged the expansion of ATM, internet and mobile banking have made financial access affordable and accessible for large numbers of residents.

The transformation however, has been most significant for India's urban, non-poor residents. These policies have not addressed the unique challenges the poor face in financial access, and they consequently, remain at the periphery when it comes to effective access to finance.

The UID-enabled micropayments solution is just one of the many developmental applications that the UID number can enable. It is also a critically important application, which can help address India's financial divide. Linking the UID number to a universal, accessible, and affordable micropayments model can transform the access the poor have to banking services in the country.

UID-enabled micropayments can be a stepping stone to creating economic opportunities for residents across the country, regardless of where they live. The financial inclusion that it makes possible will be critical to improving access for the poor to resources and skills. As we move towards an open access society, it is this soft infrastructure — connectivity, financial inclusion, and identity — that will ultimately, empower the individual in India.



Resident Data Security within Aadhaar System

Security at the Time of Enrolment

Use of standard enrolment software provided by UIDAI with built-in security and quality check features.

Operators have Aadhaar, are trained and certified before they start enrolment. And ALL enrolment packets are biometrically signed by the operator ensuring traceability and non-repudiation.

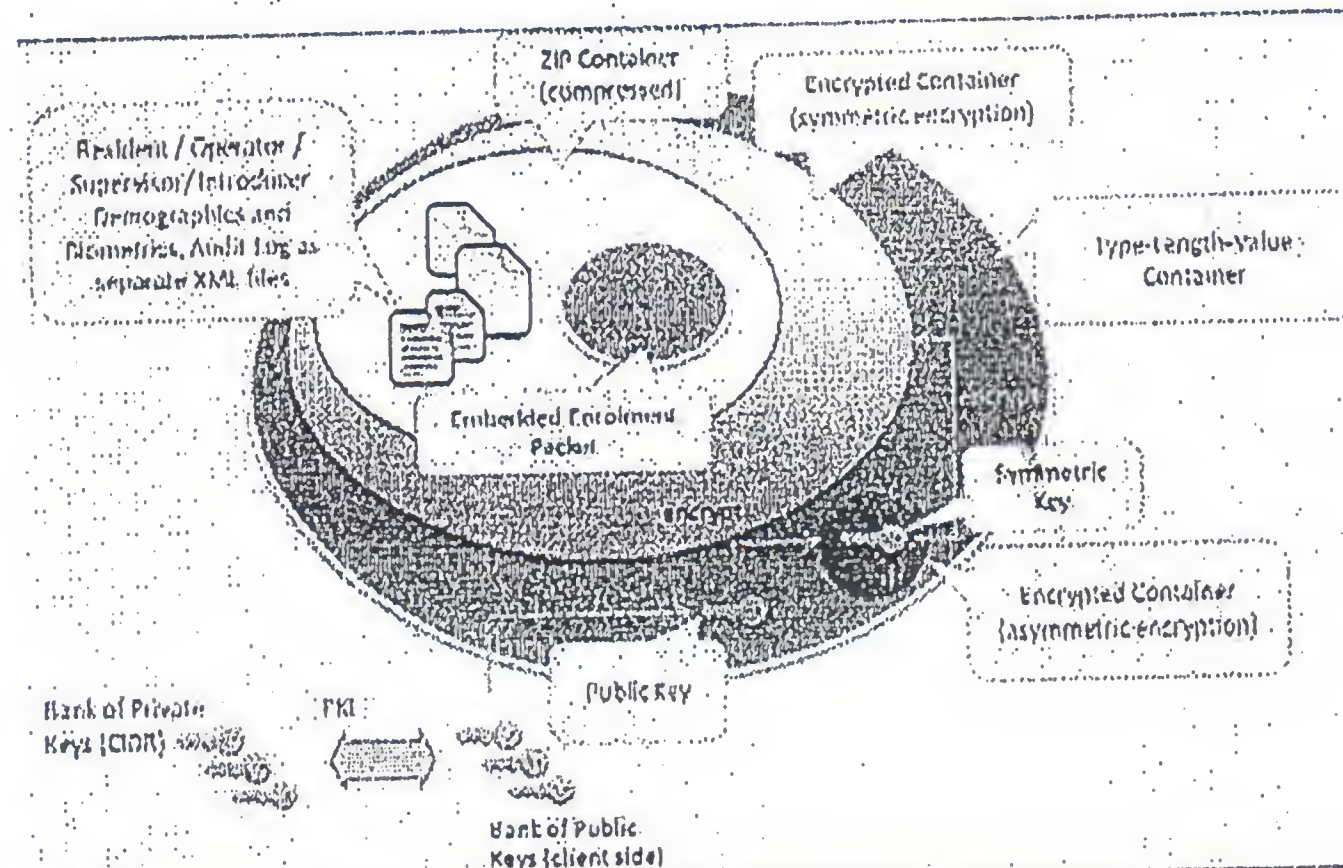
Enrolment packet is reviewed by a supervisor for data quality and signed biometrically.

The application ensures that resident data including biometrics is encrypted before it is saved to disk. Once encrypted, only CIDR can decrypt them as the private keys are with UIDAI only.

The 2048 bit PKI encryption ensures that it is IMPOSSIBLE to decrypt and steal any information even if enrolment packets are available.



Resident Data Packet Structure



3

Security in Transit

Every enrolment data packet is "always" stored in PKI encrypted, tamper proof files and cannot be decrypted ever in transit.

The enrolment packets can be uploaded only through Aadhaar SFTP Client having strong access controls.

Enrolment data is "never" decrypted until it has reached within UIDAI's data centre's secure production zone.

Metadata such as "time spent on demographic data screen", "number of corrections done" etc are collected as part of every enrolment packet for analysis of operator actions.

4

Security in Data Centre

Entire data center including ALL data within all systems is managed by UIDAI

Physical security with biometric access controls

Logical security by partitioning data centre into 'zones' separating them using firewall and network intrusion detection and prevention systems.

Complete isolation of Demilitarized Zones (DMZ), Partner DMZ, Staging, Production, and sub zones within production for biometric systems, quality check system, databases etc.

5



Security in Data Centre

Use of HSM (Hardware Security Module) and standard security practices ensures

All data "access" are controlled using common access control scheme managed within internal LDAP (Light Weight Directory Access Protocol)

Multi-vendor firewall, Network Intrusion Detection and Prevention systems, virus and malware detection systems - in the eventuality of any security compromise, it is limited to one zone.

Resident raw packet NEVER stored without high strength encryption

6



... Security in Data Centre

Biometric and non-biometric validation of "all" enrolment packets for authenticity of source, authenticity of operators and overall validity of data.

Every sub-system including the three biometric de-duplication systems are separated by firewalls.

Data is "partitioned" across multiple security "zones", meaning "no" single database has all the resident data in completeness.

Biometric data provided to biometric sub-systems (that are deployed within UIDAI data centres) are fully anonymized (biometric system does not ever know whose biometric is being processed)



In the Indian context, there is a need for UID for better monitoring and targeting of social benefits and employment programmes and, at the same time, identifying synergies between various ID Initiatives prevalent. The UID system would ensure that residents need not prove they exist every time they interface with the Government or the private sector.

1.2 The Vision

UID would be a unique number used for *identification* of the residents of India for various statutory, administrative, developmental and commercial purposes.

The Unique ID would provide an easy and common means of identification of all the residents of the country by all government agencies, thereby enhancing efficiency, transparency, reliability and effectiveness at affordable costs to the common person in the delivery of public services. This, in turn, would authenticate every person's right to government services and benefits through a single system rather than all government departments investing in creating infrastructure, systems and procedures for verification of residents under various schemes of the Government.

The UID would enable better monitoring and targeting of social benefits and employment programmes. On an overall basis:

- It would be the common unique identifier for residents
- the UID would act as a conduit to improve targeted delivery of the fruits of a growing economy to the common person, and
- It would aim at eliminating the need for multiple identification mechanisms prevalent across government departments.

Vision Statement

Creating a unique identification system of all residents in the country for efficient, transparent, reliable and effective delivery of various welfare and private services to the common person.

1.3 Unique ID and its Benefits

It is envisaged that the UID, together with the socio-economic data, would enhance:

- Efficiency and effectiveness of the social sector schemes
- Convenience and quality of public service
- Improvement in service delivery system, and
- Transparency in administration

The key benefits to be realized by the Government, residents and the private sector are as listed below:

A. Benefits to Government

- The UID would enable various government departments to leverage an easy and reliable beneficiary identification mechanism
- It would help in building on the existing identification mechanism, leading to overall efficiency gains in governance and better delivery
- Reduce identity-frauds across the country
- Once implemented, the UID would eliminate the need for creating elaborate beneficiary-identification mechanisms and, in turn, would reduce duplication of efforts across Government machinery
- With robust beneficiary identification mechanisms and cross-referencing of databases, the UID would support the Government of India in better (targeted) policy-formulation under various schemes and programmes
- Overall, the UID would help in improving transparency in administration

B. Benefits to Residents

- Reduce hassles in their interactions with multiple Government departments for establishing their identification

- Ensure convenience in availing various services - both public and private
- The UID number would act as a single window for residents to establish their identity and avail benefits

C. Benefits to Private / NGO Sector

- Private sector would be able to leverage the resident identification infrastructure and, in turn, contribute to effective development activities
- Use UID to speed up certain businesses, especially in the insurance and credit sectors
- May eliminate the need for the private sector to set-up parallel identification systems leading to improved efficiency in delivery of their services
- A reduction in identity-related frauds in the service delivery

52 117
ANNEXURE R-4

Annexure VII

Ministry of Communications & Information Technology
Department Information Technology
Electronics Governance Division

Electronics Niketan,
6-CGO Complex,
New Delhi 110003
March 3, 2006

ADMINISTRATIVE APPROVAL

Subject: Administrative approval for the project - "Unique ID for BPL Families".

I am directed to convey the Administrative Approval of the Competent Authority for implementation of the project - "Unique ID for BPL Families" at a total estimated outlay of Rs. 46.70 crores (Rupees Forty Six crores and Seventy Lakhs only) for a duration of 12 months to be implemented by NIC through NISLI. The total amount of Rs. 46.70 crores is to be released from DIT as grant-in-aid to be met from e-Governance programme. The details of the project are given at Annexure-I.

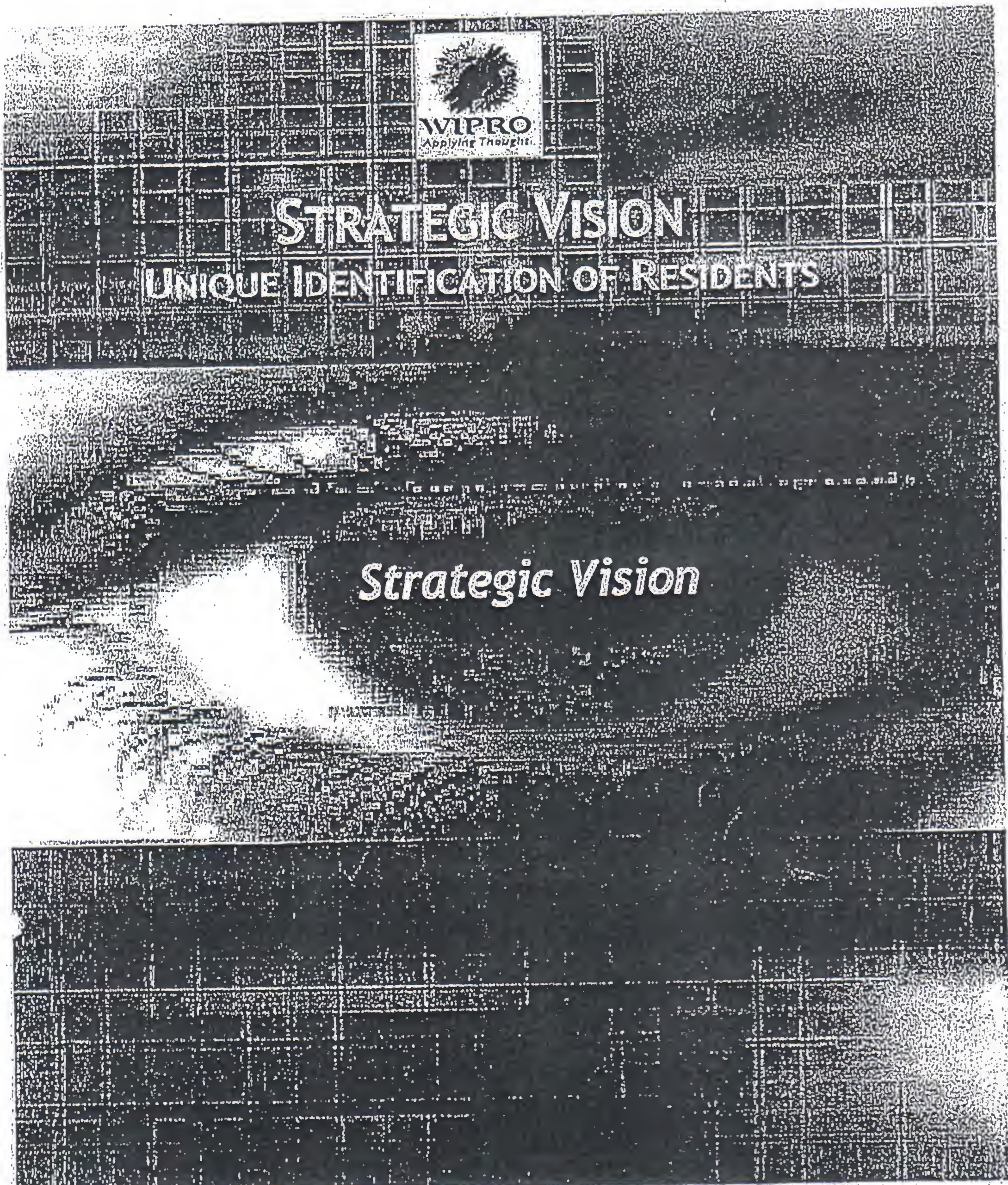
This issues with the approval of Hon'ble Minister (MC&IT) vide diary no. 8383 dated 6.02.2006 and concurrence of JS&FA vide diary no.8383 dated 21.2.2006.

K. Bidani
(Krishna Bidani)
Deputy Director

Copy to:

1. Pay. & Accounts Office
2. Drawing & Disbursing Section (2 copies)
3. Deputy Financial Advisor, Integrated Finance Division, DIT
4. The Principal Director of Audit Scientific Department, I.P. Estate, New Delhi.
5. The Managing Director, NISLI, 6th Floor, NBCC Tower, 15 Bikaner place, New Delhi, With a request to furnish the acceptance of the terms and conditions of Grant-in-Aid and Administrative Approval.
6. Director General, NIC
7. Senior Technical Director (Ms. Rama Nagpal), NIC
8. Shri R. Chandrashekar, Joint Secretary, e-Governance Group, DIT.
9. SD (SSG)/ Dir (SA)/ JD (MMK)/ DD (KB).
10. Sanction File.

K. Bidani
(Krishna Bidani)
Deputy Director



STRATEGIC VISION UNIQUE IDENTIFICATION OF RESIDENTS

Strategic Vision

nISg National Institute for Smart Government
Strategic Planning, Project Consulting, Capacity Building

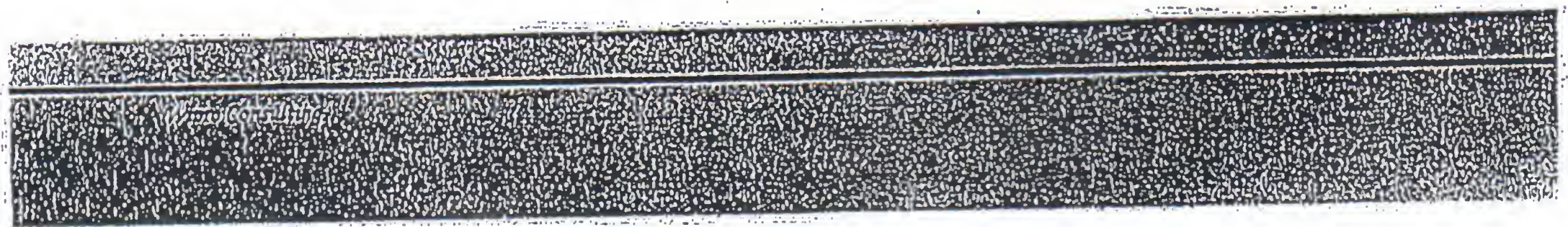
Department of Information Technology
Ministry of Communications & Information Technology
(Govt. of India)





Table of Contents

| | |
|--|----|
| Preface | 3 |
| 1. Strategic Vision..... | 5 |
| 1.1 Rationale for UID..... | 5 |
| 1.2 The Vision | 6 |
| 1.3 Unique ID and its Benefits | 7 |
| 2. Strategic Dimensions for the Success of UID..... | 9 |
| II.1 Applicability and Accessibility of UID..... | 9 |
| II.2 Intensive Usage and Validation | 9 |
| II.3 Leverage Collective Strength of Government | 10 |
| II.4 Linkages with other Databases | 10 |
| II.5 Processes..... | 11 |
| II.6 Statutory Mandate | 11 |
| 3. Realizing the Vision - Mission and Objectives | 12 |
| III.1 Short Term Mission | 12 |
| III.2 Medium Term Mission | 13 |
| III.3 Long Term Mission | 14 |
| III.4 Snapshot across Time Horizons..... | 16 |
| 4. Ownership and Capacity Building | 17 |
| 5. Implementation Challenges..... | 18 |
| 6. Conclusion..... | 19 |





Preface

Project Unique Identification is a Planning Commission, Government of India (GoI) initiative, steered by the Department of Information Technology-GoI, with the objective of creating a central database of information on residents and assigning a Unique Identification (UID) number to each resident in the country, as the basis for efficient delivery of welfare services.

UID would authenticate every person's enlistment for government services and benefits through a single centralized system rather than each government department or agency investing in infrastructure, systems and procedures for identifying residents under its schemes, individually and independently. UID would facilitate a common proof for residence and identity over period of time.

To this end, the project envisages incorporating UID as part of existing databases thereby providing for linkages with all such databases to the central UID database, as well as providing for future additions to the content-fields of the database by the user-agencies as per their requirements.

One of the key advantages envisaged as an outcome of the project is that the Unique ID will help in reducing identity-related frauds and allow only targeted persons to avail of benefits from the government.

Given the diversity in requirements of the user-agencies, a Vision Workshop was held to brainstorm on the UID initiative and provide inputs for the Project, on 21 November 2006. The workshop examined similar initiatives being implemented at the State level, discussed the vision, and mission for the project (detailed in this document) and arrived at a common understanding of the purpose of, and approach to, the Process Study. This document is intended to lay down the Strategic intent for the initiative.



based on the summarization of the deliberations of the vision workshop and various Central and State Government Departments.

Implementing agencies, for the proposed initiative, include NICS/NIC, as the technical solution provider for the creation, generation and operation of the central UID database and Wipro, as consultants to the Process Committee, chaired by the Principal Adviser, Planning Commission, to design the UID and an associated information system that is based on the UID, and also to define the processes for creation and maintenance of the UID as well as the administrative procedures and user manuals.

1. Strategic Vision

1.1 Rationale for UID

In human life cycle, there is a need for government services at various stages and at each stage, the unique resident ID can act as an identifier through which services can be provided to the authorized person.

At present, various government departments are investing in creating infrastructure, systems and procedures for verifying entitlement claims of residents under various schemes and initiatives of the Government (PAN, Passport, Voter ID, Driving License, etc.). From the resident's point of view there is a need to ascertain that services reach the right persons. From the department's point of view, it is a time-consuming exercise to create and maintain their own database, which is a duplication of efforts, and could be avoided had there been a single database. However, such a database does not exist, nor is there any mechanism for different departments to share a universal database to identify the resident.

In fact, efforts of all agencies (Election Commission, Ministry of Rural Development, Office of the Registrar-General of India, Public Distribution System, and so on) are "stand-alone" and "one-off" and hence efforts so far are not leveraged optimally.

Many countries use a unique identification number as a means of tracking their permanent and temporary residents for the purposes of work, National ID, taxation, government benefits, health care, and other government related functions (driver's license, passport, payroll, e purse, etc.). The ways in which such systems are implemented is specific to each country, but in most cases, a resident is issued a card at birth or when they reach a legal age (typically the age of 18).

In the Indian context, there is a need for UID for better monitoring and targeting of social benefits and employment programmes and, at the same time, identifying synergies between various ID initiatives prevalent. The UID system would ensure that residents need not prove they exist every time they interface with the Government or the private sector.

1.2 The Vision

UID would be a unique number used for identification of the residents of India for various statutory, administrative, developmental and commercial purposes.

The Unique ID would provide an easy and common means of identification of all the residents of the country by all government agencies, thereby enhancing efficiency, transparency, reliability and effectiveness at affordable costs to the common person in the delivery of public services. This, in turn, would authenticate every person's right to government services and benefits through a single system rather than all government departments investing in creating infrastructure, systems and procedures for verification of residents under various schemes of the Government.

The UID would enable better monitoring and targeting of social benefits and employment programmes. On an overall basis:

- it would be the common unique identifier for residents
- the UID would act as a conduit to improve targeted delivery of the fruits of a growing economy to the common person, and
- it would aim at eliminating the need for multiple identification mechanisms prevalent across government departments.

Vision Statement

Creating a unique identification system of all residents in the country for efficient, transparent, reliable and effective delivery of various welfare and private services to the common person



1.3 Unique ID and its Benefits

It is envisaged that the UID, together with the socio-economic data, would enhance:

- Efficiency and effectiveness of the social sector schemes
- Convenience and quality of public service
- Improvement in service delivery system, and
- Transparency in administration

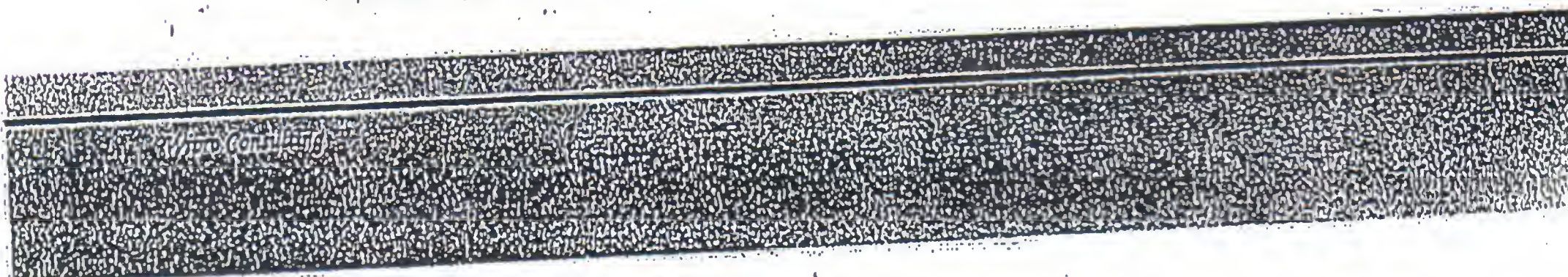
The key benefits to be realized by the Government, residents and the private sector are as listed below:

A. Benefits to Government

- The UID would enable various government departments to leverage an easy and reliable beneficiary identification mechanism
- It would help in building on the existing identification mechanism, leading to overall efficiency gains in governance and better delivery
- Reduce identity-frauds across the country
- Once implemented, the UID would eliminate the need for creating elaborate beneficiary-identification mechanisms and, in turn, would reduce duplication of efforts across Government machinery
- With robust beneficiary identification mechanisms and cross-referencing of databases, the UID would support the Government of India in better (targeted) policy-formulation under various schemes and programmes
- Overall, the UID would help in improving transparency in administration

B. Benefits to Residents

- Reduce hassles in their interactions with multiple Government departments for establishing their identification





- Ensure convenience in availing various services - both public and private
- The UID number would act as a single window for residents to establish their identity and avail benefits

C. Benefits to Private / NGO Sector

- Private sector would be able to leverage the resident identification infrastructure and, in turn, contribute to effective development activities
- Use UID to speed up certain businesses, especially in the insurance and credit sectors
- May eliminate the need for the private sector to set-up parallel identification systems leading to improved efficiency in delivery of their services
- A reduction in identity-related frauds in the service delivery

2. Strategic Dimensions for the Success of UID

It is envisaged that, for better acceptance of UID across the country by residents, Government departments and the private sector, the following cornerstones are deemed pre-requisites:

II.1 Applicability and Accessibility of UID

To start with, UID should be used for effective implementation of the social sector schemes outlined in the 11th Plan. At the same time, the UID initiative should also look at taking a mixed approach to social services and neutral services based on the readiness of the implementing States. This would help in checking malpractices, better selection of bonafide beneficiaries and ensuring that benefits reach them, thus checking leakages in the system and improving delivery mechanism.

Due emphasis would be on making UID number easily accessible to both residents and Government or its agencies without compromising on security aspects.

II.2 Intensive Use and Validation by Multiple Agencies to Achieve Accuracy over Time

Fresh data collection and validation is a tedious, expensive, time-consuming and error-prone process. Conversion into digital format is an arduous task that introduces additional inaccuracies and fresh cost and time implications. Accuracy and perfection of data is, and will remain, a continuing challenge in this complex exercise. Yet, speed is important. Therefore, it is intended to use an existing data base available in electronic and bilingual format, namely the electoral roll data base, while being fully cognizant of its current limitations regarding accuracy, currency and completeness of data.

It is envisaged that intensive usage and validation of the resident data by multiple agencies would achieve higher accuracy levels over a period of time.

II.3 Leverage Collective Strength of Government (Technology-Enabled Collaboration)

The basic premise for the success of UID is the concept of "one owner, many users." Practically, each department would be in a position to add and own any field required for its purpose backed up by 100 percent foolproof tracking of all modifications.

In this regard, technology would play a central (crucial/vital ??) role in the use of UID by various departments. Technology-enabled seamless integration across departments would ensure widespread use of UID and continuous validation of the database by leveraging the collective strength of the Government.

II.4 Linkages with other Databases

Linkage of UID database with other databases would ensure continuous updation and use-based validation. This could be ensured by a 'symlotic' linking of all other major databases to UID and vice versa for delivery of services / benefits.

In this direction, the Election Commission's database would be used as the base database; however, some links between UID and the Election Commission's database may be maintained for cross-referencing. At a later date, it is envisaged that UID and Multi-purpose National Identity Card (MNIC) may converge.

Further on, for all future Census and sample surveys, the UID would be indicated in the Identification Block of the structured questionnaire for data



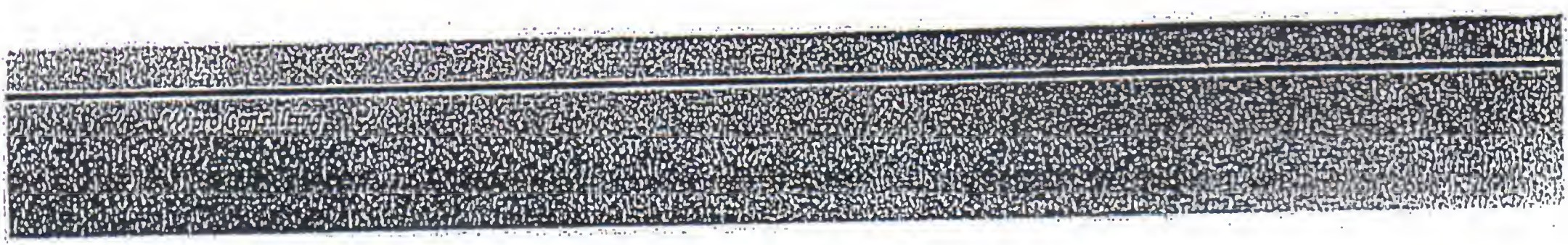
collection and it is suggested that the Registrar-General of India (RGI) would leverage UID for the 2011 census data.

II.5 Processes

For the successful adoption of UID, it would be imperative to build robust processes to update the UID data continuously and, at the same time, opportunities for continuous updating of varying data would have to be explored. For this, transactions from existing systems would have to be linked to UID, by ensuring enthusiastic participation of stakeholder departments.

II.6 Statutory Mandate

Importantly, statutory backing would be required for the adoption of UID by residents, Government departments, its agencies and the private sector in the long term.





3. Realizing the Vision - Mission and Objectives

In order to realize the envisaged vision, it is suggested that a phased approach be adopted with clear objectives for the following time horizons:

- Short Term
- Medium Term
- Long Term

III.1 Short Term Mission (3 Years) - Use of the UID for Specific Schemes (BPL) in Identified States

A. Stakeholders

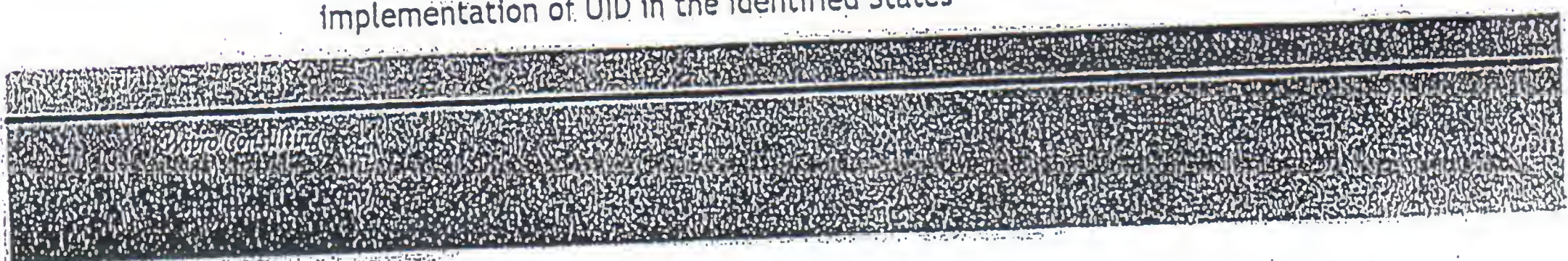
Adopting a phased approach for the implementation of the UID across the country, starting with potential users of UID would be select Government departments (implementing BPL schemes), identified States and beneficiaries of the selected BPL schemes.

Key expectations of the departments, at this stage, would be evaluating the practicality of implementation of UID for specific schemes; establishing the linkage between UID and BPL databases across Identified States and tracking delivery of benefits to bonafide beneficiaries. On the other hand, residents would look forward to better service delivery with easier access to benefits.

B. Pre-requisites

For the mission to be achieved in the specified timeframe, the pre-requisites would include:

- Centralized availability of the Election Commission's resident data post-data-cleansing
- Identification of an appropriate custodian / owner of the UID database
- Establishment of the required institutional framework for implementation of UID in the Identified States





C. Key Objectives

In the initial stages of implementation, the UID initiative would strive to attain the following objectives:

- Assign Unique ID from existing digital database of the Election Commission (for residents 18 years of age and above)
- Create awareness about the initiative amongst potential users
- Establish linkages between UID database and the BPL database
- Facilitate UID adoption in the implementation of welfare schemes
- Establish institutional mechanism for administering the UID and build appropriate capacity
- Authorize and authenticate resident data across the country for use by various departments

III.2 Medium Term Mission (5-7 Years) - State-wide Implementation and Use of UID for Major Schemes

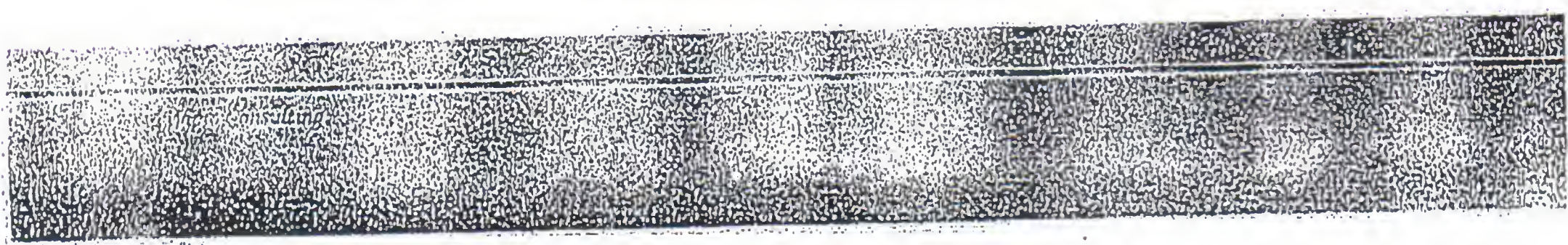
A. Stakeholders

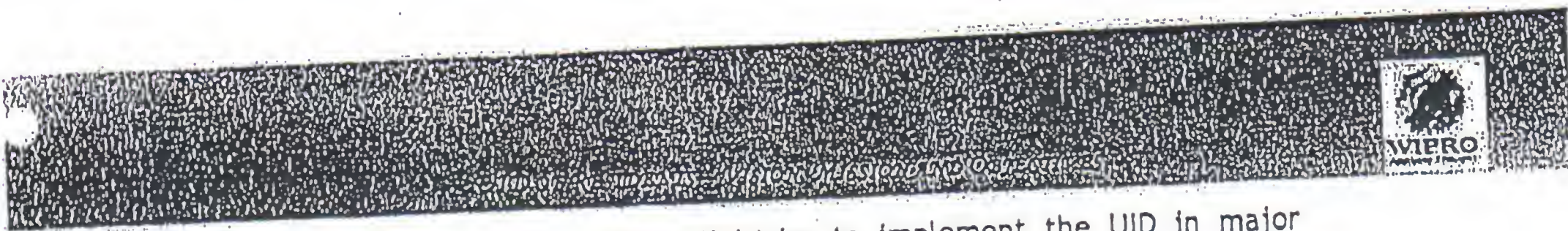
In the medium term, the key stakeholders would be most of the Government departments, majority of State Governments and all the beneficiaries of Government schemes and services.

Key expectations of the Government departments from the UID initiative in the medium term would be a wider coverage of residents eliminating the need for investment in parallel resident identification infrastructure by individual departments. At the same time, residents would prefer the UID to act as an acceptable and authentic identification mechanism for the majority of services entitled to them.

B. Pre-requisites

To achieve State-wide usage of UID and adoption of the same for delivery of the schemes, some of the pre-requisites would include:





- Building capacity across Ministries to implement the UID in major schemes being implemented by them across the country
- Establishing institutional mechanism for resident verification

C. Key Objectives

The key objectives for the UID initiative in the medium term would include:

- Assigning Unique ID to all residents.
- Completing all preparatory work for implementation of UID for all major schemes in all States
- Evolving procedures for maintenance and updating of UID and facilitating linkage of UID database with other major databases
- Implementing UID for majority of schemes in as many States as possible
- Enhancing efficiency, transparency, reliability and effectiveness in the delivery of public services
- Facilitating cross linkages (two-way linkages) of UID database with the databases of other departments

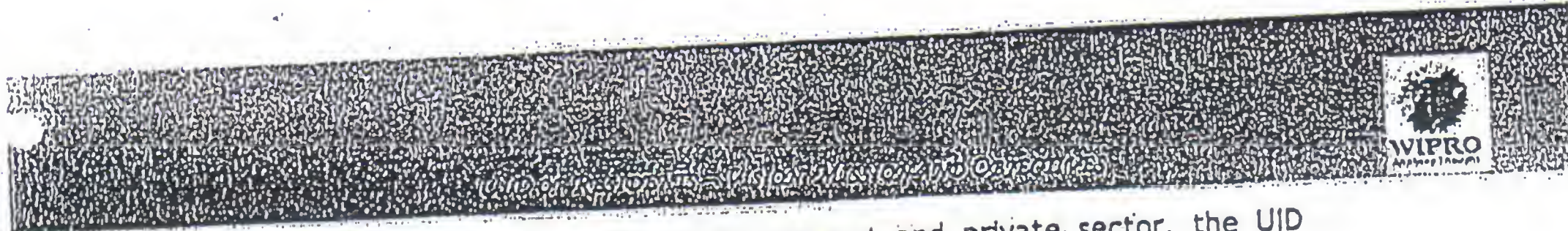
III.3 Long Term Mission (10 Years) - Make the UID as the de-facto Identifier for all Residents in the Country

A. Stakeholders

It is envisaged that, in the long term, UID would transform into being a *de facto* Identifier for all residents of the country. In this scenario, potential users of UID would be all the residents and all Government and private agencies needing authentication of resident identity prior to delivery of service.

For the residents, the key expectation from this initiative would be the elimination of the requirement of carrying multiple identification proofs for accessing various services during his/her lifespan ensuring better, faster and more transparent delivery of services.





For the service providers, both Government and private sector, the UID initiative would eliminate the need for investing huge sums of money in establishing the identity of the recipient of services and in preventing identity-frauds.

B. Pre-requisites

For realizing the long term mission, some of the pre-requisites would include:

- All residents below 18 years of age are also brought into the UID database, since the Election Commission's database (the primary source for the UID database) accounts only for residents above 18 years of age
- Executive and legislative mandate for all service providers (Government and private) to deem the UID number as THE universal identifier for service delivery

C. Key Objectives

Key objectives in the long term would include:

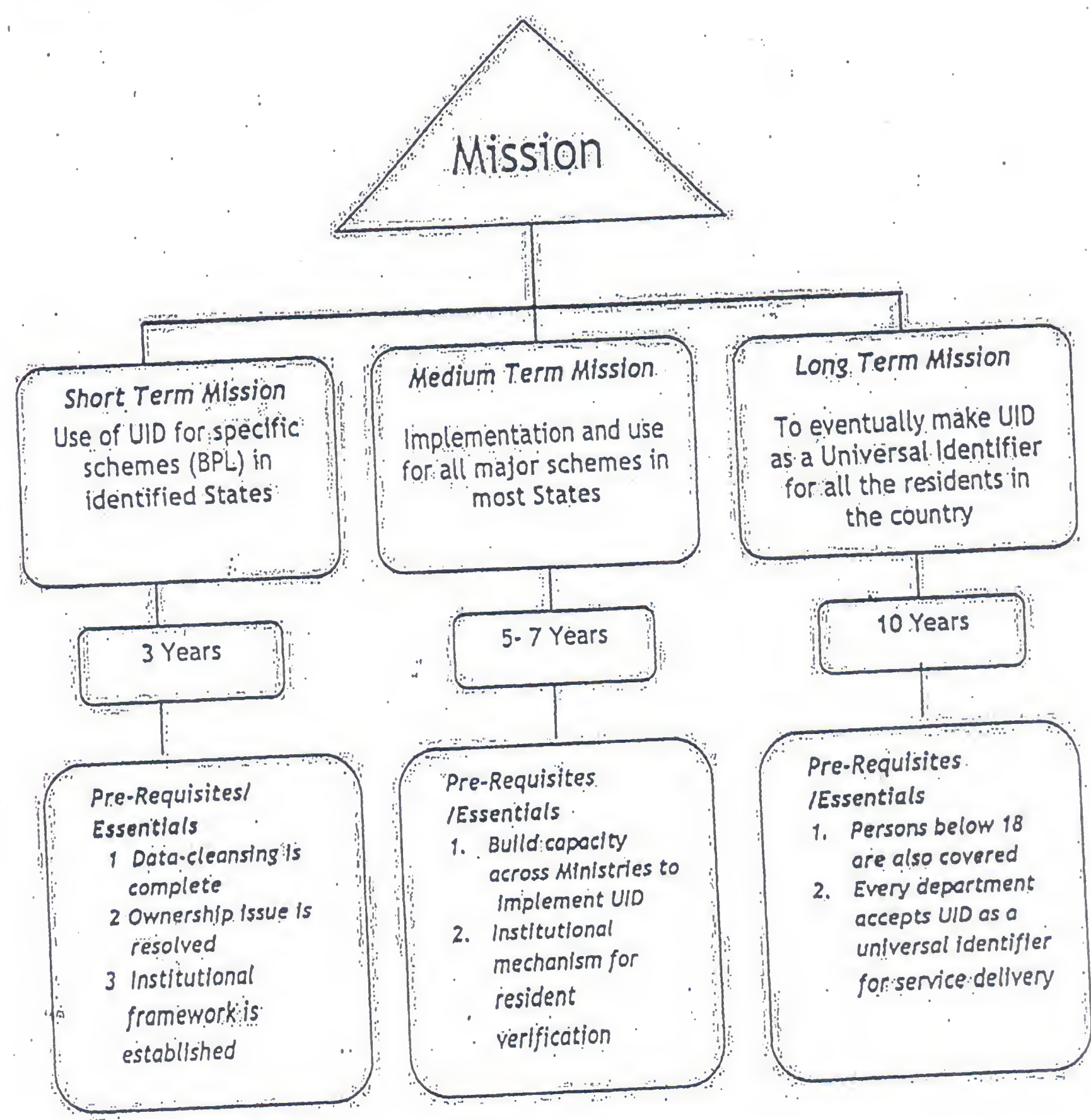
- Implementation of the UID in all citizen-centric service delivery as the universal identifier
- Introducing the UID in all the Ministries, departments and to all private service providers as the only identifier





III.4 Snapshot across Time Horizons

As highlighted above, phased approach for UID adoption and implementation across India would include:





4. Ownership and Capacity-Building

For the success of a national-level initiative like the UID, there is an immediate need for identifying or establishing an appropriate Authority for administering UID initiative and be the custodian and owner of the two major components of UID:

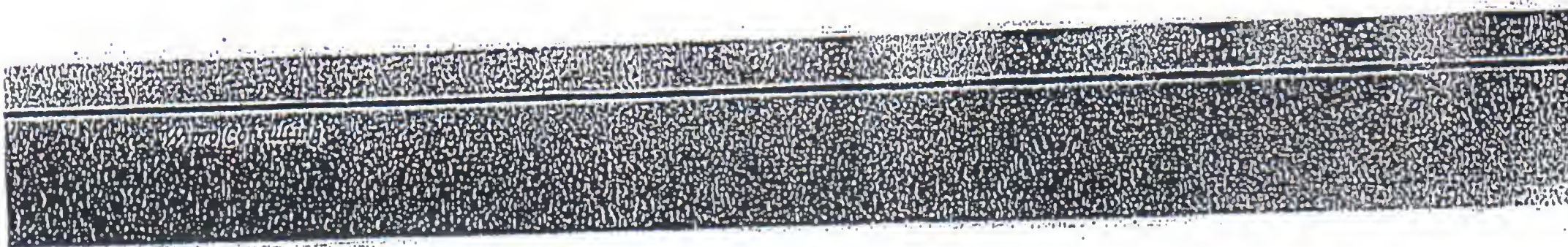
- Core Database
- Application Database

In respect to the core database, this agency may be an existing entity capable of administering the UID across the country; conversely, it could be a new agency equipped with the requisite institutional framework and legal mandate to administer the UID system across various States.

It is envisaged that the application databases would be maintained by the respective departments and the said departments would continue to be the owners of their respective application databases.

Given the international perspective on similar initiative, capacity-building would be a critical element to ensure the success of the UID initiative. Capacity-building initiatives would have to be implemented for:

- Owners of the core database
- Owners of the application databases
- User-departments

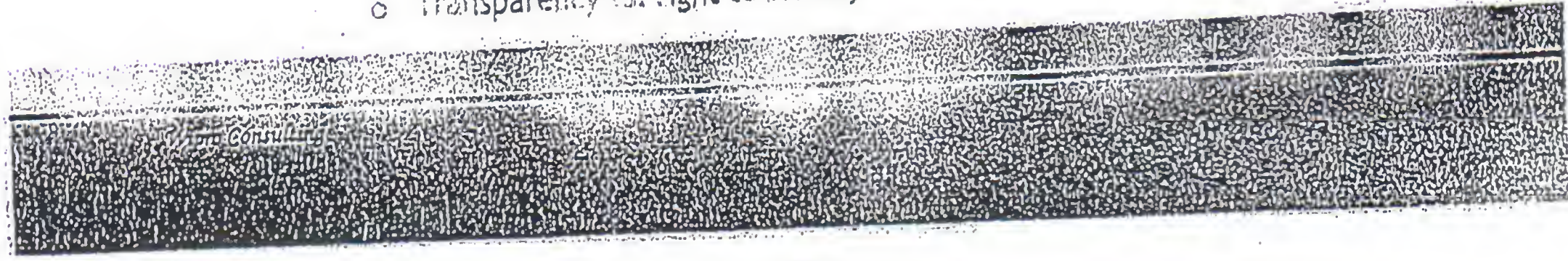




5. Implementation Challenges

There have been many Unique ID initiatives across the world that has yielded mixed results. While some have failed, others have had limited success. In the Indian context, some of the key implementation challenges foreseen include:

- Change management within the Government machinery and residents across the length and breadth of the country is seen as the biggest challenge to the adoption of UID
- Setting up governance structures for implementation at various levels may take a long time before it becomes fully operational, leading to loss of momentum and zeal for implementation
- Creating and maintaining infrastructure in a vast and diverse country such as India could turn out to be a challenge in itself
- Standardizing geographical (habitation / villages) codes, applications, databases and processes, keeping localization requirements in mind, would require a thorough appreciation of the dynamics of a diverse nation like India
- Security and privacy. This would require a lot of focus and conviction to ensure adoption by different stakeholders
- Complexities involved in establishing linkages between UID and other major databases would be critical for adoption of UID by other Departments
- Addressing the limitations of the Election Commission's data and building on the same would be a challenge in itself
- Some other challenges to be addressed would include:
 - Ease of use vs. tight control/security
 - Departmental control vs. collaboration among departments
 - Rigorous procedures vs. convenience of individuals
 - Rapid adoption vs. manageable phasing
 - Transparency vs. right to privacy



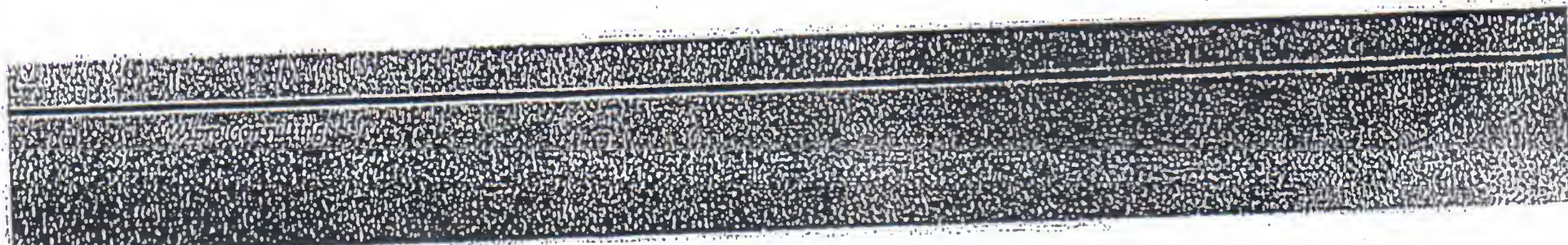
31
136



6. Conclusion

Given the pathbreaking perspective as envisaged in the vision for the proposed UID Initiative and the complexities involved, there is a need to undertake the UID Initiative on a Mission Mode.

The UID Initiative should ultimately encompass multiple linkages although it may have limitations in the near-short term. However, it envisages the linking the whole country in a not-too-a-future by assigning a unique identification number to each and every resident which he/she can use achieving the same through short-term / medium term and long-term objectives while assigning UID for each resident in a phased manner.



72
137

Annexure VIII

List of attendees of Vision Workshop Dated 26th of November, 2006.

| NAME | DESIGNATION | DEPARTMENT |
|--------------------------|-------------------------|---|
| Shri B.K. Chaturvedi | Cabinet Secretary | |
| Shri. Rajeeva Ratna Shah | Member Secretary | Planning Commission |
| Dr. Arvind Virmani | Principal Advisor | Planning Commission |
| Shri Jalinder Singh | Secretary | Department of Information Technology |
| Dr. Renuka Viswanathan | Secretary | Ministry of Rural Development |
| Shri Ramachandran | Secretary | Ministry of Urban Development |
| Shri R. Chandrashekhar | Additional Secretary | Department of Information Technology |
| Shri D.K. Sikri | Registrar General | Registrar General of India |
| Smt Anita Chaudhary | Joint Secretary | Department of Food |
| Dr. B.K. Galrola | Director General | National Informatics Centre |
| Vaishindra Seth | | National Informatics Centre |
| Shri S. Abbasi | Director | Department of Information Technology |
| Shri Anand Prakash | Director | Department of Road Transport and Highways |
| Shri R.K. Chaturvedi | Director | Ministry of Urban Development |
| Shri G.S. Raju | Director | Ministry of Social Justice and Empowerment |
| Shri Suresh Kumar | Additional Director | Director of Income Tax CBDT (Systems) |
| Shri Y.P. Mittal | Economic Advisor | Department of School Education, Ministry of HRD |
| Shri Golak Kumar Sinhl | Senior Consultant | eGPMU, Department of Information Technology |
| Dr. Dhruvad Mathur | Senior Consultant, NeGP | Department of Information Technology |
| Smt Vineeta Dixit | Senior Consultant | eGPMU, NEGP, DIT |
| Shri Sanjay Gaden | Senior Consultant | eGPMU, NEGP, DIT |
| Smt Radha Chauhan | Principal Consultant | eGPMU, NEGP, DIT |
| Shri S.P. Singh | Senior Director | eGPMU, NEGP, DIT |
| Shri D. Krishnan | | eGPMU, NEGP, DIT |
| Shri Kumar | | Planning Commission |
| Shri Sunil Gupta | | |
| Shri Harish Kumar | | Ministry of Agriculture |
| Navneet Agarwal | Consultant | eGPMU, NEGP, DIT |
| Dr. D.K. Paliwal | | Ministry of HRD |
| Shri A. Kumar | Secretary | UNESCO |
| Shri Ghanshyam | BSF | Border Security Force |
| Shri Vivek Bharadwaj | Special Secretary | Department of Information Technology |
| Shri H Mohan | MD | Department of Food and Civil Supplies |
| Shri Sundera Sekhar | Secretary | Department of Mass Education & Extension |
| Shri G.N. Mukhopadhyay | Deputy Secretary | Department of Information Technology |
| Shri G. Mukherjee | Deputy Secretary | Food and Supplies Dept, Govt of West Bengal |
| Smt Zohra Chatterjee | Principal Secretary | Department of Industries, IT, Electronics |
| Shri Anup Pandey | Food Commissioner | Department of Food and Civil Supplies |
| Shri S.K. Singh | Deputy Commissioner | Department of Food and Civil Supplies |
| Dr. Subhash Srivastav | Deputy Commissioner | Department of Rural Development |

73
138

Annexure VIII

| | | |
|---------------------------|-------------------------|---|
| Shri S C Jain | Assistant Director - IT | Centre of egovernance, DIT |
| Shri R. Singh | Special Consultant | |
| Shri Kaushik Mukherjee | Principal Secretary | Department of Higher Education |
| Shri Rajeev Chawla | Secretary | eGovernance |
| Shri B. H. Anil Kumar | Commissioner | Department of Food and Civil Supply |
| Shri Anil Kumar Jha | Project Administrator | Department of Health |
| Shri K. M. Makhwana | Under Secretary | Department of Food and Civil Supplies |
| Ms Neeta Shah | Director | e-Governance |
| Shri S. N. Rao | General Manager | Department of Food, Civil Supplies and Consumer Affairs |
| Shri S. R. Rao | General Manager | State Civil Supplies Ltd |
| J. Satyanarayana | CEO | NISG |
| Mahabaleshwar Hegde | Vice President | NISG |
| Shri Phaneendra Vinnakola | General Manager | NISG |
| Sameer Sachdeva | Relationship Manager | NISG |
| Arpita Khare | Manager Projects | NISG |

(RASHTRAPATI BHAVAN)
RASHTRAPATI BHAVAN

New Delhi, the 4th December, 2005
Agrahayana 13, 1928 (S)

Subject: Constitution of an Empowered Group of Ministers (EGoM) to collate two schemes – the National Population Register under the Citizenship Act, 1955 and the Unique Identification Number Project of the Department of Information Technology.

It has been decided, with the approval of the Prime Minister, to constitute an Empowered Group of Ministers (EGoM) to collate two schemes – the National Population Register under the Citizenship Act, 1955 and the Unique Identification Number Project of the Department of Information Technology. The EGoM may also look into the methodology and specific milestones for early and effective completion of the Project and take a final view on these.

2. The composition of the EGoM, as approved by the Prime Minister, will be as under :-

Shri Pranab Mukherjee,
Minister of External Affairs;
Shri Shivraj V. Patil,
Minister of Home Affairs;
Shri H.R. Bhardwaj,
Minister of Law & Justice;
Shri Mani Shankar Aiyar,
Minister of Panchayati Raj, Minister of Youth Affairs &
Sports and Minister of Development of North Eastern Region; and
Shri Dayanidhi Maran,
Minister of Communications & Information Technology.

Special Invitee

Shri Montek Singh Ahluwalia,
Deputy Chairman, Planning Commission.

3. The Empowered Group of Ministers (EGoM) will be serviced by the Department of Information Technology.

(K.L. Sharma)
for Cabinet Secretary
Tele: 2301 5344

To

Shri Pranab Mukherjee, Minister of External Affairs.
Shri Shivraj V. Patil, Minister of Home Affairs.
Shri H.R. Bhardwaj, Minister of Law & Justice.
Shri Mani Shankar Aiyar, Minister of Panchayati
Raj, Minister of Youth Affairs & Sports and
Minister of Development of North Eastern
Region.
Shri Dayanidhi Maran, Minister of Communications
& Information Technology.
Shri Montek Singh Ahluwalia, Deputy Chairman, Planning Commission.

KC

SECRET

Annexure XI

DRAFT

Minutes of the first meeting of the EGoM to collate two schemes-the National Population Register (NPR)/MNIC under the Citizenship Act 1955 and the Unique Identification number (UID) project of the Department of Information Technology (DIT).

Date: 27-11-2007
Venue: 162, Committee Room South Block
Time: 18:30 PM
Participants: List attached

1. The Chairman initiated the proceedings by welcoming the members of the EGoM. He briefly enunciated the purpose and scope of the EGoM, which is to consider and devise mechanism for collating the two projects.

He referred to the two sets of data - one focused on citizens (under the MNIC project) and the other covering residents (under UID project).

He appreciated the efforts of MHA in implementing the MNIC pilot, the learnings from which would certainly facilitate further understanding and appreciation of issues that essentially needed to be addressed at the national level for implementing an identity project.

He underlined the need and importance of a verifiable and credible database of individuals that would enable efficient and effective delivery of benefits to eligible individuals. In this context, he referred to the UID database that has been created based on the voter list of the Election Commission of India (ECI), which is the most credible and validated data on residents available in the country.

76

141

Annexure XI

2. This was followed by a presentation on the UID project by Shri R. Chandrasekhar, Additional Secretary DIT, and on the MNIC/NPR project by Shri D.K. Sikri, Additional Secretary and RGI.

Salient features highlighted in the two presentations included:(I) UID:

- (i) Building upon existing data of residents (voter list), incrementally.
- (ii) Establishing linkages with major database holders such as MoRD, PDS, ECI, and RGI.
- (iii) Leveraging technology to enable collaborative and intensive usage of the database by multiple agencies, to ensure extensive coverage and accuracy.
- (iv) Establishment of an authority both at the Centre and State(s) that will own, manage, maintain and operate the database as per laid down processes and forge ongoing linkages with identified agencies.
- (v) Initial linkage with ECI being established.

(II) MNIC/NPR:

- (i) The Pilot Project for test checking of processes and technology almost completed in selected areas in 12 States and one Union Territory in the country. Distribution of identity (smart) cards to citizens in border as well as non-border areas is in progress.
- (ii) The Pilot Project has helped establish the technical specifications and technology for personalisation of identity (smart) card indigenously. The card security against cloning has been ensured thru' the Key Management System developed by NITC.

Annexure XI

- (iii) Creation of National Population Register (NPR) of all the Residents with a single reference date at Census 2011 is recommended. National Register of Indian Citizen (NRIC) can be prepared as a byproduct asynchronously depending on the need. Entries subsequent to the date in the NPR would be subject to verification of citizenship.
- (iv) De-novo creation of NPR is not recommended and it should be done alongwith Census 2011 to apportion costs. Cost of NPR creation will be lower if identity cards are given on demand and payment in non-border areas.
- (v) Data handling and management as well as it's updating at tehsil/ block level thru' local service centres (6000 in number) by linking them to births and deaths, is administratively feasible.
- (vi) The NPR so created and updated thru' births/ deaths, can usher in Register based census in the country.
- (vii) The interregnum upto 2009 be utilised to develop indigenous technologies in areas which are in proprietary domain. Capacities in plastic and chip production are likely to be set up in the country once the intention of the government about the national roll-out is known.
- (viii) The identity card besides being a tool for identification for providing benefit/ service, can become a multi- application card by increasing the memory size of the chip.

3. Remarks by Members:

(I) Shri. Shiyra V. Patil, Minister of Home Affairs:-

He pointed out that the information under the NPR/Census, relating to residents, can be collected only by the RGI and should be used for creating the identity database. DIT and its agencies can provide technology assistance for its updating and maintenance mechanism.

Annexure XI

An independent and dedicated institutional mechanism / Authority should be created which is entrusted with ownership of the database and made responsible for its updation and maintenance on an ongoing basis.

He also pointed out to the flexibility that is available with reference to the information that can be stored in the cards issued to residents. For instance, additional information relating to specific areas such as borders, hills, sparsely populated regions etc. can be stored in the cards for ready reference.

(II) Shri A. Raja Minister of Communications and Information Technology

He stated that the need for such an initiative is clearly established. It is now imperative that the efforts under the two projects are synergized, since they have the common purpose of creating an identity database of residents. He suggested that the most practical approach would be to host the database on computer systems and enable access by authorized persons/ agencies by enabling connectivity.

He also emphasized the need for establishing an authority (a dedicated institutional mechanism) that would be responsible for regulating operations and maintenance of the database post its creation, since this aspect will assume central importance in the entire exercise that is being embarked upon.

(III) Shri Montek Singh Ahluwalia Deputy Chairman Planning

Commission:

In the context of the major and persistent issue that Planning Commission is faced with relating to effective targeting and reaching of welfare

Annexure XI

benefits to eligible individuals under various government schemes and programmes, it would be useful to have smartcards based on UID.

He opined that the most practical and immediate way would be to build on the UID database, which is already in place, especially in view of the XIth Plan objectives.

(IV) Panchayati Raj: Shri. B.K. Sinha, Additional Secretary Panchayati Raj (representing the Minister) stated that the Panchayati Raj Institutions (PRIs) are major creators as well as users of data relating to residents in their jurisdictions. Their role in the whole scheme should effectively use their pivotal and constitutional position as the third tier of government.

Under the ePRI project that has been initiated by the PR ministry in consultation with DIT, it is envisaged that village level (Gaon Sabhas) panchayats will be equipped to digitize and operate data at the village itself. This factor should be duly taken into account, while deciding the institutional mechanism for operation and maintenance of the resident database.

(V) Secretary DIT, apprised the members about the meeting held by the Union Home Secretary to consider issues relating to collation between the two schemes and the emergence of some suggestions on the approach that could be adopted in this regard. A note based on this deliberation is being finalized and will be placed before the EGoM at its next meeting. He also mentioned that a Detailed Project Report for creation of Central and State UID authorities has been supported by the Planning Commission 'in principle'. This shall also be placed, formally, before the EGoM in the next meeting.

80
145

Annexure XI

4. The Chairman's concluding remarks:

- (I) It has clearly emerged that there is a need for creating an identity related resident database, regardless of whether the database is created based on a *de novo* collection of individual data or is based on already existing data such as the voter list and there is a critical and imperative need to identify and establish an institutional mechanism that will 'own' the database and will be responsible for its maintenance and updating on an ongoing basis post its creation.
- (II) The mechanism and processes that the Institution would have to put in place to update and maintain the database will impact the overall effective implementation and achievement of outcomes that are being envisaged under the two projects.
- (III) In this context, the next meeting of the Group will need to consider:
 - (i) Methodology to be adopted for collation of the two schemes.
 - (ii) Ways for effective implementation and use of the database.
 - (iii) Identification of an institutional mechanism that will 'own' the database and will be responsible for its maintenance, updating and usage on an ongoing basis post its creation.
 - (iv) Time schedule for operationalising the scheme/s.

-:000:-

81
146

Annexure XI

Participants at BCOM:

1. Shri Pranab Mukherjee (Minister of External Affairs)
2. Shri Shivraj V. Patil (Minister of Home Affairs)
3. Shri A. Raja (Minister for Communications & Information Technology)
4. Shri Montek Singh Ahluwalia (Dy. Chairman - Planning Commission)
5. Shri Madhukar Gupta (Secretary - Ministry of Home Affairs)
6. Shri Jainder Singh (Secretary - Department of IT, Ministry of Communications & Information Technology)
7. Shri B. K. Sinha (Additional Secretary - Ministry of Panchayati Raj)
8. Shri R. Chandrashekhar (Additional Secretary - Department of IT, Ministry of Communications & Information Technology)
9. Shri D. K. Sircar (Registrar General of India, Ministry of Home Affairs)

P

Annexure XI

Minutes of the Second Meeting of EGoM to collate two schemes - the National Population Register (NPR/MNIC) under the Citizenship Act, 1955 and the Unique Identification number (UID) project of the Department of Information Technology (DIT)

Date: 28.01.2008

Venue: 9, Parliament House

Time : 4.30 P.M.

Participants: List attached

1. The Chairman initiated the proceedings by welcoming the members of the EGoM. He recapitulated the four key issues that were identified for further consideration in the first meeting of the EGoM (held on 27th Nov. 2007),

- i. Methodology to be adopted for collation of the two schemes
- ii. Ways for effective implementation and use of the database
- iii. Identification of an Institutional mechanism that will 'own' the database and will be responsible for its maintenance, updating and usage on an ongoing basis post its creation.
- iv. Time Schedule for operationalising the scheme/s.

He mentioned that the Agenda Note that has been tabled for consideration of the EGoM covers the strategy for collation between NPR and UID (based on the deliberations held by Home Secretary) as also the institutional mechanism that would own and operate the UID database post its creation. The presentation that will be made before the Group would, in addition to the agenda note, cover issues relating to

Annexure XI

alternative implementation, usage and the time schedule for operationalising the scheme.

It was also indicated that after the presentation, certain issues may need to be clarified such as progress of the MNIC pilot project and status of setting up of one lakh Common Service Centres (CSC). This would enable a realistic assessment of preparations that would be needed for NPR enumeration and collation of the two schemes.

2. The opening remarks of the Chairman were followed by a presentation by Additional Secretary DIT, Shri. R. Chandrashekhar. Copy of the presentation was circulated to the members. At the request of Home Secretary, a note on 'Effective implementation and use of data base along with Institutional mechanisms for its management and maintenance' prepared by MHA was circulated to members with the permission of the Chair.

The salient features of the presentation by Additional Secretary DIT included:

- i. Background of MNIC and UID
- ii. Strategy for collation of UID and NPR (as detailed at Annexure I to these minutes)
- iii. Establishment of UID Authority
- iv. Approvals sought

Annexure XI

In addition to the above, the presentation outlined the phased implementation model of UID based on linkages with partner databases, the possible approach to usage of UID/NPR database and the proposed time schedule for the scheme.

Approval was sought for the strategy proposed for collation between NPR and UID schemes and in principle approval for establishment of the UID Authority under the Planning Commission.

3. Following the presentation, the Minister of Home Affairs, Shri Shivraj V. Patil observed that the proposal to collect photographs and biometrics (for NPR) separately and subsequent to primary enumeration should be reexamined and suggested that the primary enumeration under NPR exercise ought to include collection of photographs and biometrics and only those who are left out in the primary round should be covered separately and subsequently.

The RGI explained that the MNIC pilot has indicated practical difficulties in collecting biometrics and photographs in a single round of enumeration; necessarily, on an average, complete capture of photo and biometrics for a household involved a minimum of 3 rounds, hence the proposal for asynchronous capture of photo and biometrics so that the NPR enumeration could adhere to the census timelines.

The Home Secretary assured that the option suggested by the Home Minister would be examined particularly in the light of the 1 lakh CSCs

85

150

Annexure XI

that are being set up across the country under the DIT scheme. Accordingly the NPR proposal could factor in capturing of biometrics and photographs during primary enumeration under NPR to the extent feasible without affecting the timelines for Census.

Additional Secretary, DIT, informed that to date contractual arrangements for 72,000 CSCs with a 12 month implementation timeline have been finalized and for the rest, contracting is expected to be completed by March 2008. Accordingly by March 2009, it is expected that the CSCs will be physically operational and the infrastructure available therein could be leveraged for collection of photographs and biometrics for the NPR.

Home Secretary proposed that a pilot be undertaken immediately, to test the feasibility of incremental enumeration under NPR.

Minister of Panchayati Raj, Shri Mani Shankar Iyer, pointed out that the Panchayati Raj Institutions (PRIs) constitute a major arm of Government machinery with close contact with people at the field level, particularly at the village level. He therefore suggested, that the PRIs at the ground level ought to be formally involved to play a pivotal role in the enumeration exercise that would be undertaken by the MHA for NPR specially with regard to collection of photographs and biometrics as well as for validating the data collected and in subsequent activities.

4. After the discussions, the Chairman summarized the decisions of the EGoM, namely:



86
151

Annexure XI

- i. Strategy proposed for collation of NPR and UID was approved.
However, primary enumeration under NPR exercise could include collection of photographs and biometrics to the extent feasible without affecting Census timelines and only those who are left out in the primary round could be covered separately and subsequently.
- ii. Proposal to establish UID Authority under the Planning Commission was approved.
- iii. Planning Commission would ensure necessary approvals within the timelines indicated for creation and establishment of the UID authority.
- iv. In principle approval was accorded for conducting pilot to test and work out feasibility of incremental enumeration under NPR.
- v. CSCs should be utilized
 - (a) for collection of photographs and biometrics for NPR,
 - (b) for electronic data entry under NPR (from the filled schedules) to the extent considered appropriate and feasible.
- Pilot (as approved above) should include these aspects also while testing the feasibility of incremental enumeration.
- vi. The implementation of UID as per timelines annexed (Annexure II) was approved.
- vii. The PRIs should be appropriately leveraged, to the maximum extent feasible, in collection of data for NPR/UID as well as its validation while cross linking with the designated agencies.

Annexure XI

SECRET

Annexure IStrategy for Collation of UID and NPR

- UID expected to be in place by June 2008
- NPR exercise would be undertaken to the extent needed excluding biometrics & photo along with Census 2011
- Primary enumeration during NPR exercise to build incrementally upon UID database, to the extent feasible
- ORG & DIT to undertake a Pilot / POC to determine feasibility of enumeration using UID database
- In case this is not found feasible, data collection would need to be undertaken de novo
- Resultantly, UID number would be transposed on the NPR database
- ~~Data collected under NPR would be handed over to UID Authority for maintenance & updation~~
- NPR could thus become a partner (collaborative) database in the UID scheme



88
153

Annexure XI

SECRET

Annexure II

Time Schedule for the Scheme

| No. | Milestone | Date |
|-----|--|-------------------------------------|
| 1. | In-principle approval of EGoM for establishment of UID Authority under Planning Commission | Jan 2008 (Step 1) |
| 2. | Approval of UID Scheme | March 2008 (Step 1 + 2 months) |
| 3. | Notification of UID Authority | April 2008 (Step 1 + 3 months) |
| 4. | UID Generation and Allocation | June 2008 (Step 1 + 5 months) |
| 5. | Linkage with MoRD/PDS Databases | June-Dec'08 (Step 1 + 11 months) |
| 6. | UID ready for collation with NPR | April 2009 (Step 1 + 15 months) |



Annexure XI

S. (SECRET)

List of Participants:

1. Shri Pranab Mukherjee, Minister of External Affairs
2. Shri Shivraj V. Patil, Minister of Home Affairs
3. Shri H. R. Bhargava, Minister of Law & Justice
4. Shri Mani Shankar Aiyar, Minister of Panchayati Raj
5. Shri A. Raja, Minister of Communications & Information Technology
6. Shri Montek Singh Ahluwalia, Dy. Chairman - Planning Commission
7. Shri Madhukar Gupta, Secretary - Ministry of Home Affairs
8. Shri Jainder Singh, Secretary - Department of Information Technology
9. Shri R. Chandrashekhar, Addl. Secretary - Department of Information Technology
10. Shri D. K. Sikri, Registrar General of India

DRAFT

Minutes of the Third Meeting of the EGoM to collate two schemes- the National Population Register (NPR/MNIC) under the Citizenship Act, 1955 and the Unique Identification Number (UID) project of the Department of Information Technology (DIT)

Date: 07-08-2008
Venue: 162, Committee Room South Block
Time: 18:30 PM
Participants: List attached

1. The meeting began with the Chairman inquiring about the progress of NPR. On this Secretary, Ministry of Home Affairs (MHA) briefed the members on the action taken and progress so far, with reference to the directions of the EGoM at its second meeting. He stated that the schedule for NPR to be canvassed along with census 2011 is under finalisation. At the same time, ground work on pilots for testing the feasibility of incremental enumeration of NPR based on UID has been initiated. Fourteen locations spread across six States have been identified for the purpose of the first pilot/PoC. Field enumeration is proposed to be taken up in September and would be completed within a month. Schedules and their formats for the enumeration during the PoC have been finalised.
2. Deputy Chairman, Planning Commission (PC) referred to the decision of the last (2nd) meeting of the EGoM wherein PC had been directed to prepare a proposal for establishment of the UID Authority. He stated that while comments of Finance Ministry on the proposal, circulated at the meeting, need to be examined but on the issue of nature of the nature UID Authority of India (UIDAI), it may come into being as an executive body initially but it will have to become independent later as a statutory entity. He requested that the members may take up the proposal for substantive consideration in the EGoM and then seek final approval of the

Prime Minister. This submission was followed by a presentation of the proposal by Adviser, PC Dr. C. Muralikrishna Kumar.

3. Salient features of the presentation included strategies for covering non adult residents as the present concept covers age group of 18 years and above based on the ECI database. This can be done through specific initiatives for covering the residents in the age group 0 - 18 years through the creation of the National Students' Register to capture the age group 6-18 years, ICDS and NRHM data for capturing age group 0-5 years and a National Birth & Death Register. These would flow from the existing initiatives undertaken by respective Ministries/Departments. In addition, creation of Unique Identity for Geographic Locations (UIG) is a necessary counterpart of the UID for individuals as individuals have a root and are linked to place of birth and /or place of residence. Creation of an Asset Register for development deliverables would help in better targeting and arrest leakages of funds for developmental activities. The presentation also enumerated on aspects like Field verification, enumeration and validation; the Governance structure, institutional framework for the UID Authority of India; Broad activities & timelines; financial requirements and the Specific approvals sought from the EGoM.

4. Remarks by the Members

(i) Shri Shivraj V. Patil Minister of Home Affairs

He expressed his general endorsement of the core objectives, overall design and approach of the scheme and the proposal of the PC for establishment of the UID Authority. Since the Home Minister was to leave for another meeting, he assured his support to whatever was decided by the EGoM

(ii) Shri A. Raja Minister of Communications and Information Technology

While expressing his agreement with the proposal, he referred to the DIT's comments on the proposal circulated at the meeting, and suggested that the PC may indicate a specific date by which the UID would be available to an initial set of users for delivery of welfare services to the residents. He also suggested that the field verification for establishing linkage

between the UID database on the one hand and the BPL and PDS databases on the other, should be done concurrently and not separately in view of the time and cost of the effort as well as logistical convenience.

(iii) Shri Mani Shankar Iyer, Minister of Panchayat Raj

He drew attention of the members to the minutes of the last EGoM in particular to para 4 (vii) pertaining to leveraging of PRIs to the maximum extent feasible in collection, validation of data and its cross linking with databases of other designated agencies. He reiterated that while the objective of covering all residents is commendable, PRIs involvement in the whole scheme has to be incorporated and institutionalised as they are closer to the field reality. Adoption of appropriate strategies is therefore, essential for leveraging PRIs optimally and to this extent, an expert in PRIs must be made a member of the proposed National Advisory Body of the Authority.

He stated that it must be appreciated that Panchayat Raj Institutions at the field level are ideally suited to handle field level verification and validation and in most states they are already notified as the agency for registration of births and deaths. Instead of over dependence on the bureaucratic machinery there must be a systemic shift towards the panchayat setup keeping in view their open and participatory processes of decision making. Credibility and ownership of the UID processes (which should include updation of data by PRIs post its creation) would be enhanced with the involvement of the PRIs. Referring to the Gairola Committee Report he also mentioned that all PRIs would be interconnected enabling complete transparency of their working and fund utilisation. The Plan Plus application developed by NIC would enable all data relating to a village and its development being made available on a single platform.

Referring to the proposed Unique Geographical Identifier (UGI) and codification of regions up to habitation level he expressed hope that this would help in operationalising the provisions of the Panchayat (Extension to the Scheduled Areas) Act, wherein village is defined as a habitation, more accurately and

effectively. A comprehensive Asset Register (as indicated in the proposal) at the village level will also be of great value in management and identification of assets locally.

He concluded by stating that the UID superstructure could be well served by the PRIs at the field level if this suggested strategy is adopted.

(iv) Shri H.R. Bhardwaj Minister of Law & Justice

He observed that the proposal of the PC is comprehensive and it would be prudent to establish the authority first and the modalities and funding pattern can be worked out subsequently, as in view of the federal structure of the country, the States would also have to be consulted and involved. He stated that the EC data is well tested and is certainly mature enough for use as proposed.

(v) Shri Montek Singh Ahluwalia Deputy Chairman Planning Commission

In response to some of the observations made during the discussions, the Deputy Chairman PC, averred that the question of whether the authority should be under the aegis of PC or not, is an issue that EGoM had decided and the present proposal has been tabled as per the direction of EGoM. The Planning Commission was not averse to the whole initiative including the proposed UIDAI being brought under the purview of any other ministry or organization. A strategic decision needs to be taken whether to build the UID progressively on existing databases such as Electoral Roll/EPIC and BPL in a manner that would feed into the NPR as and when it comes into existence (thereby enabling a double check on the NPR) or to wait till the NPR comes into being as the mother database in 2013 and thereafter put in place linkage processes to operationalise UID.

He emphasised the tremendous benefits that could flow out of register based UID - be it tracking of movement of residents, conferment of benefits of government programmes in a targeted manner or monitoring of their credit profile by Financial Institutions. He emphasised that this initiative is very critical for modernising the country as a whole, and in this context he also

mentioned the recent launch of the Rashtriya Swasthya Bima Yojana where beneficiaries would be provided with smart cards for availing of health related benefits on similar lines that is envisaged under the UID scheme.

He agreed to the suggestion of the Minister Panchayati Raj that the UID Authority could include PRI experts. On the observation that the proposed structure was top heavy he stated that PC was open and willing to consider any suggestions in this regard.

5. Other remarks:

Secretary, MHA reiterated his agreement with the overall approach to convergence of UID with NPR as agreed upon at the last meeting of the EGoM. However, he was of the view that the present proposal has projected a far wider scope than what was initially envisaged and this needed to be examined as some parts of it did not appear to be necessary. He drew particular attention to an element in the proposal tabled by the PC that presently nonexistent databases would be created and developed under the aegis of the UIDAI. He felt that this appeared unnecessary and could impact the UID timelines adversely. Secretary, MHA further opined that the proposed structure of the UIDAI seemed top heavy and could be suitably pruned.

He proposed that the MNIC /NPR project of the MHA would be implemented over the next two to three years alongside the census operations. Comprehensive data collected as part of the NPR should become the mother database with photographs and finger biometrics of each individual, which could then be utilised by various agencies to deliver benefits. Whether efforts should be undertaken to build new departmental databases such as National Students Register, National Birth and Death Register etc. in the meanwhile to make UID data more comprehensive, was an issue that needed to be examined and considered. The mother database of NPR, once in place, could then be updated by PRIs through the 100,000 Common Service Centres one each for a group of 5-6 villages that DIT would be establishing across the country under the National

eGovernance Plan. It would be pertinent at that point of time to consider whether the UID authority should have a statutory basis or not. The establishment of UIDAI then as a statutory authority would need to be perceived along with the extant provisions of the Indian Citizenship Act, under which the RGI is the National Registration Authority. Any independent statutory arrangements envisaged for UID would need to take these existing provisions into account.

Secretary PC submitted that UID- MNIC-NPR data would provide a comprehensive coverage of the residents. The proposal tabled by PC is to establish UID by building on the existing databases that have been identified and to seed Electoral/EPIC data with UID to serve as a basis for incremental enumeration under NPR to the extent feasible. The alternative is to not do anything now and wait for the NPR to be made available after 2013 before operationalising the UID. He mentioned the vast sums of money running into lakhs of crores of rupees that the government was spending on various welfare and social sector programmes and the need for more efficient and effective targeting that the UID would enable. He was of the view that it was not advisable to wait till NPR was ready and whatever action was considered feasible and desirable in the meantime should be taken.

Referring to the observation of Minister PR relating to the creation of an asset register, he clarified that the register is envisaged as a by product of the UID Initiative that could be built by any user department for its use.

He reiterated that as pointed out in the proposal, UIG and personal identification once in place will greatly impact the efficiency and effectiveness of government delivery system. The Authority can be anchored initially in the PC as an interim arrangement and later can become independent.

On the suggestion of MoC & IT of when UID would be available for use be clearly indicated, he clarified that ideally this should

be possible by April, 2009 but keeping practical problems that could arise on the ground, it would be more realistic to aim for Sept 2009 as the timeline by which the UID can be put to limited use based on its initial linkage with Electoral Roll/EPIC data.

On the suggestion of conducting concurrent field verification and linkage of UID with BPL and PDS he agreed that the suggestion would optimise time and effort and stated that as it is for States to decide on the modalities of this exercise, we could consider directing the States to take up the exercise concurrently as far as possible.

6. Chairman's Concluding Remarks

Concluding the discussion, the Chairman appreciated the proposal drafted by the PC and observed that it is comprehensive in content. The source data for covering the residents exhaustively has also been elaborately laid out.

He pointed out that many important issues have been raised by the members present and in the written comments conveyed by the Finance Minister and other various ministries involved. He also commented on the need for examining the role of PC with reference to the proposed UIDAI in light of the ARC recommendations of 1965.

The resolution of some of these issues (as compiled and annexed to the minutes as Annexure) would require detailed and in depth discussions which could more appropriately be had by an official level committee. He directed that a Committee of Secretaries should examine the various issues raised and give its recommendations to the EGOM to facilitate a final decision in the matter *on the earliest*.

[Signature]

UID ISSUES TO BE RESOLVED BY COS

1. Should the UIDAI be a statutory or executive authority?
 - a. If statutory, at what stage - Initially or later?
 - b. If statutory, how would this role be reconciled with statutory role of National Registration Authority under Citizenship Act?
2. Should the supplementation of ECI data in respect of under 18 residents be undertaken by UIDAI building directly or indirectly, National Register of Students, National Register of children/Infants and National Register of Births and Deaths OR should this additional information be extracted as a sub-set from the NPR being compiled by RGI as and when it is ready?
3. What should be the specific role of PRIs in line with the decision of the 2nd EGOM?
4. Should the scope of activities of UIDAI cover the following extended set of activities proposed by PC?
 - a. NRS
 - b. NRC
 - c. NRB&D
 - d. National Register of Assets
 - e. Unique Geographical Identity Code up to habitation level
5. Should the UIDAI be established under the PC in view of ARC recommendations of 1965 giving PC only a recommendatory role? If not under PC, under which ministry/ department/ organization/ authority should it be anchored?
6. Is the staff size of the UIDAI proposed justified? Is the superstructure appropriate?
7. Should the UIDAI at central and state levels be a central authority as envisaged in the proposal of the Planning Commission or should it follow the ECI basic framework in respect of structure at central and state level as well as the relationship between central and State set up?
8. What should be the target date for the UID to be made available for usage by an initial set of authorised users?
9. Should the cross-verification of UID with BPL and PDS be carried out simultaneously or sequentially? Should the linkage with BPL be done with existing data of BPL Survey of 2002 or proposed BPL Survey of 2007 (yet to be undertaken)?
10. Procedure to be adopted for obtaining approval of UIDAI
 - a. EGOM or
 - b. EFC - CCEA

List of Participants :

1. Shri Pranab Mukherjee, Minister of External Affairs
2. Shri Shivraj V Patil, Minister of Home Affairs
3. Shri H R Bharadwaj, Minister of Law & Justice
4. Shri Mani Shankar Aiyar, Minister of Panchayati Raj
5. Shri A Raja, Minister of Communications & Information Technology
6. Shri Montek Singh Ahluwalia, Dy. Chairman- Planning Commission
7. Shri Subas Pani, Secretary Planning Commission
8. Shri Madhukar Gupta, Secretary- Ministry of Home Affairs
9. Shri Jainder Singh, Secretary- Department of Information Technology
10. Shri R Chandrashekhar, Addl. Secretary- Department of Information Technology
11. Shri D K Sikri, Registrar General of India
12. Smt. Rita Menon Addl. Secretary - Ministry of Finance

Minutes of the Fourth Meeting of the EGoM to collate two schemes-the National Population Register (NPR/MNIC) under the Citizenship Act, 1955 and the Unique Identification Number (UID) project of the Department of Information Technology (DIT)

Date: 04-11-2008

Venue: 162, Committee Room south Block

Time: 16.00 PM

Participants: List attached

1. The Chairman initiated the meeting by stating that the objective of the Empowered Group of Ministers (EGoM), was to collate the two schemes-the National Population Register (NPR/MNIC) under the Citizenship Act, 1955 and the Unique Identification Number (UID) project. Recalling the past proceedings and decisions of the EGoM, he referred to the decision in the 2nd meeting to set up the UID Authority (UIDAI) under the Planning Commission (PC) with the direction to the PC to ensure necessary approvals within timelines indicated for creation and establishment of the UIDAI.

Pursuant to this decision, the PC had placed before the EGoM a detailed proposal for setting up UIDAI which was considered in the last meeting i.e. the third meeting held on 07-08-2008. Consequent to the deliberations of the EGoM on the proposal, ten issues were referred to the Committee of Secretaries (COS) headed by the Cabinet Secretary, to examine the issues raised and give its recommendations to the EGoM to facilitate a final decision in the matter.

He informed the members that the recommendations of the COS are now placed for consideration and requested the members to take up for consideration each of the issues along with the recommendations to arrive at a final decision.

2. Shri R. Chandrashekhar, Special Secretary, Department of IT with permission of the Chair presented the recommendations of the COS on each of the ten issues referred to it.

Issue 1

Should the UIDAI be a statutory or executive authority? If statutory, at what stage - initially or later? If statutory, how would this role be reconciled with statutory role of National Registration Authority (NRA) under Citizenship Act?

COS Recommendation:

Initially UIDAI may be notified as an executive authority, as proposed. The issue of investing the UIDAI with statutory authority and the reconciliation of such statutory role with NRA can be taken up for consideration later at an appropriate time, if found necessary.

Decision of JCoM: Recommendation of COS was approved.

Issue 2

Should the supplementation of ECI data in respect of under 18 residents be undertaken by UIDAI building, directly or indirectly, National Register of Students, National Register of children/ infants and National Register of Births and Deaths OR should this additional information be extracted as a subset from the NPR being compiled by RGI as and when it is ready?

COS Recommendation:

UIDAI may limit its activities to creation of the initial database from the Electoral Roll/EPIC data and verification and validation of the same through BPL and PDS data and updation of electoral rolls. UIDAI may not directly undertake creation of any additional database but will find appropriate systems to supplement the UID database. UIDAI may however additionally issue instructions to agencies that undertake creation of databases, to ensure standardization of data elements that are collected and digitized to enable collation and correlation with UID and its partner databases.

Decision of EGoM: Recommendation of COS was approved.

Issue 3:

What should be the specific role of PRIs in line with the decision of the 2nd EGoM?

COS Recommendation:

UIDAI will take its own decision as to how to build the database. They may have to refer to many institutions for the same. PRIs should be leveraged to the maximum extent feasible in validation of data and its cross linking with databases of other designated agencies

Decision of EGoM: Recommendation of COS was approved

Issue 4

Should the scope of activities of UIDAI cover the following extended set of activities proposed by PC? (a) NRS, (b) NRC (c) NRB&D, (d) National Register of Assets and (e) Unique Geographical Identity Code (UIG) up to habitation level.

COS Recommendation:

Issues (a) to (d) have been clarified in recommendations on Issue 2.

UID may be operationalised with UIG upto village level, initially. As and when UIG upto habitation level becomes available it may be incorporated in the UID database.

Decision of EGoM: Recommendation of COS was approved

Issue 5

Should the UIDAI be established under the Planning Commission (PC) in view of ARC recommendations of 1965 giving PC only a recommendatory role? If not under PC, under which ministry/ department/ organization/ authority should it be anchored?

COS Recommendation:

In view of the fact that the project has a pan departmental scope and objective and Planning Commission is the only agency that deals with most departments, it was decided that UIDAI be anchored in Planning Commission as proposed.

Decision of EGoM: Approved the COS recommendation with the stipulation that this decision would be valid for five years and thereafter, a view could be taken by the Government on where the UIDAI would finally be located within the Government.

Issue 6

Is the staff size of the UIDAI proposed justified? Is the superstructure appropriate?

COS Recommendations:

It was decided that the Committee will not go into the details of the proposal at this stage. Approval for the complete structure and full contingent of staff may be processed through DoE and CCEA as per normal procedure. However, approval of EGoM may be sought for constitution of UIDAI with a small, lean core team (upto 10 personnel) initially.

Decision of EGoM: EGoM accepted the recommendation of COS and accorded its approval to the constitution of the UIDAI with a core team of 10 personnel at the central level including one officer at the level of Additional

Secretary to the Government of India, one officer at the level of Joint Secretary to the Government of India and other lower level support staff.

EGoM further directed that PC should separately place the detailed proposal other than the core team with the complete structure, rest of the staff component and organisational structure of UIDAI at the central and state levels before the Cabinet Secretary for his consideration, prior to seeking approval under normal procedure through the DoE/CCFA. The EGoM directed the Planning Commission to complete this work by the end of December, 2008.

Issue 7

Should the UIDAI at central and state levels be a central authority as envisaged in the proposal of the Planning Commission or should it follow the ECI basic framework in respect of structure at central and state level as well as the relationship between central and State set up?

COS Recommendation:

UIDAI at the state level comprising of State UID Commissioner and complete staff be fully funded centrally at least for the first five years, as proposed. CEO of State UID Authority should be an officer of the level of Joint Secretary appointed by GoI from the pool of officers belonging to that particular State. Other officers could be appointed on deputation.

Staff could be appointed on contract. An Advisory Board having Chief Secretary as its chairman with Secretary (ies) - Home, Finance, Revenue, RD, Food and Chief Electoral Officer as members could be created to monitor and resolve issues. CEO State UID Authority to be Member Secretary.

Along with core staff in UIDAI at the Central level similar structure should be created in States so that work starts simultaneously at all levels.

Decision of EGoM: EGoM accepted the COS recommendation and accorded its approval to the constitution of the State UID Authorities simultaneously with the Central UIDAI, with a core team of 3 personnel including one officer at the level of Joint Secretary to the Government of India.

Issue 8.

What should be the target date for the UID to be made available for usage by an initial set of authorized users?

COS Recommendation:

It should be one year from the date of approval of the full contingent of staff for UIDAI (expected by Dec 2008). Consequently UID can be made available for use by initial set of authorized users by Dec 2009.

Decision of EGoM: Recommendation of COS was approved.

Issue 9

- 1145

Should the cross-verification of UID with BPL and PDS be carried out simultaneously or sequentially? Should the linkage with BPL be done with existing data of BPL Survey of 2002 or proposed BPL Survey of 2007 (yet to be undertaken)?

COS Recommendation:

The cross verification exercise may be taken up simultaneously to the extent possible.

Decision of ECoM: Recommendation of COS was approved

Issue 10

Procedure to be adopted for obtaining approval of UIDAI:

(a) ECoM or

(b) EEC - CCEA

COS Recommendation:

Approval of ECoM may be sought for constitution of UIDAI with a small lean core team (of upto 10 personnel) initially. On Issue 7, COS through Cabinet Secretary has recommended that similar structure should be created in the states so that work starts simultaneously at all levels. Approval for the complete

182
107
structure and full contingent of staff may be processed through EFC and CCEA as per existing procedure.

Decision of EGoM: Recommendation of COS was approved

However prior to seeking approval for the complete organisational structure and full component of staff through DoE and CCEA as per existing procedure, the Cabinet Secretary should convene a meeting to finalise the detailed organisational structure, staff and other requirements.

3. Chairman's concluding address :

(i) It also needs to be appreciated that the whole exercise being technology based and system driven, there is immense scope for outsourcing the data collation and validation work and other tasks to expert agencies in the public or private sector through a transparent process while retaining requisite control over sovereign functions. In the context, he mentioned the Passport Seva Project where retaining the sovereign functions within government (MEA), rest of the infrastructure, management and software development functions have been outsourced through a transparent process to private sector.

(iii) He stated that the UID project is unique in that the organisation (UIDAI) has to work in close collaboration with large number of institutions and agencies both within and outside government and will take at least five years to stabilize. The government at that time may need to take a fresh view particularly in light of further advancements in technology.

He concluded by appreciating the active contribution of the members and officials in the deliberations and thanked them for enabling the EGoM to expeditiously complete the work assigned to it.

List of Participants :

1. Shri Pranab Mukherjee, Minister of External Affairs
2. Shri Shivraj V Patil, Minister of Home Affairs
3. Shri A Raja, Minister of Communications & Information Technology
4. Shri Montek Singh Ahluwalia, Dy. Chairman- Planning Commission
5. Shri Jainder Singh, Secretary- Department of Information Technology
6. Shri Subas Pani, Secretary- Planning Commission
7. Shri A.N.P. Sinha, Secretary-Panchayati Raj
8. Smt. Rita Menon, Special Secretary- Department of Expenditure
9. Shri R. Chandrashekhar, Special Secretary-Department of Information Technology
10. Shri D K Sikri, Registrar General of India, Ministry of Home Affairs
11. Shri C S Kedar, Joint Secretary, Cabinet Secretariat
12. Shri Shankar Aggarwal, Joint Secretary, Department of Information Technology

New Delhi, the 22nd January, 2009

OFFICE MEMORANDUM

Subject :- Issues raised by the EGoM to collate two schemes, viz., the National Population Register (NPR/MNIC) under the Citizenship Act, 195, and the Unique Identification Number (UID) project of the D/o Information Technology.

Reference D/o Information Technology's O.M. No. 3(27)/2006-EGPMU (Pt-1), dated 26th December, 2008 regarding Governance structure, Institutional Framework, Organizational Structure and staff component of the Unique Identification Authority of India (UIDAI). While giving approval to the constitution of the UIDAI, with a core team of 115, including ten personnel at the central level including one Director General and Mission Director, and one Deputy Director General, the EGoM had directed Planning Commission to place the detailed proposal with the complete structure, rest of the staff component and organizational structure of UIDAI before the Cabinet Secretary for his consideration, prior to seeking approval under normal procedure through the DoE/CCEA.

2. The proposal has been considered by the Cabinet Secretary in pursuance of the decisions of the Empowered Group of Ministers taken in their meeting on 4th November, 2008, and it is accordingly recommended that -

- (i) the notification for constitution of the UIDAI, along with creation of the core team as approved by the EGoM be issued immediately and steps should be taken to make the Core Team operational;
- (ii) A High Level Advisory, Monitoring and Review Committee headed by Deputy Chairman, Planning Commission, consisting of following members may be constituted to oversee the work of the authority : -
 - (a) Member/Secretary, Planning Commission.
 - (b) Home Secretary.
 - (c) Secretary, D/o Information Technology.
 - (d) Secretary, Planning Commission.
 - (e) Director General & Mission Director as Member-Secretary.
- (iii) A Member, Planning Commission, or the Secretary, Planning Commission may also be assigned the task of looking after the work proposed, in the structure outlined by the Planning Commission, of the Chief UID Commissioner.
- (iv) As approved by EGoM, the Core Team consisting of Director General & Mission Director with other supporting staff may be put in place immediately. Need based creation of posts can be undertaken later after due examination in each case.

This issues with the approval of Cabinet Secretary.

(C.S. Kedar)
Joint Secretary
Tele : 23011964

To

- (i) ✓ Dr. Subas Pani, Secretary, Planning Commission



भारत का राजपत्र The Gazette of India

साप्ताहिक/WEEKLY

प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 7] नई दिल्ली, शनिवार, फरवरी 14—फरवरी 20, 2009 (माघ 25, 1930)
No. 7] NEW DELHI, SATURDAY, FEBRUARY 14—FEBRUARY 20, 2009 (MAGHA 25, 1930)

इस भाग में भिन्न पृष्ठ संख्या दी जाती है जिससे कि यह अलग संकलन के रूप में रखा जा सके।
(Separate paging is given to this Part in order that it may be filed as a separate compilation)

भाग I—खण्ड 2

[PART I—SECTION 2]

[(रक्षा मंत्रालय को छोड़कर) भारत सरकार के मंत्रालयों और उच्चतम न्यायालय द्वारा जारी की गई सरकारी अफसरों की नियुक्तियों, पदोन्नतियों व छुट्टियों आदि से सम्बन्धित अधिसूचनाएं]

[Notifications regarding Appointments, Promotions, Leave etc. of Govt. Officers issued by the Ministries of the Govt. of India (other than the Ministry of Defence) and by the Supreme Court]

राज्य सभा सचिवालय

नई दिल्ली, दिनांक 2 फरवरी 2009

सं. आरएस/1078/स्था.-कार्मिक--अधिवर्षिता की आयु प्राप्त कर लेने पर, श्रीमती प्रकाश मुंजाल, संयुक्त निदेशक 31 जनवरी, 2009 के अपराह्न से सेवानिवृत्त हो गई।

सी. बी. राय, निदेशक

योजना आयोग

नई दिल्ली, दिनांक 28 जनवरी 2009

सं. ए-4301/02/2009-प्रशा.-[--अधिकार प्राप्त मंत्री समूह की दिनांक 4 नवम्बर, 2008 को हुई बैठक के अनुसरण में, यूनिफ आईडेंटिफिकेशन ऑथोरिटी ऑफ इंडिया (यूआईडीआई) को एतद्वारा योजना आयोग के तत्वावधान में एक सम्बद्ध कार्यालय के रूप में संस्थापित और अधिसूचित किया जाता है। यूआईडीआई के विचारार्थ विषय एवं आरंभिक केन्द्रीय स्टाफ की संरचना निम्नानुसार है :--

I-452 G/2008

गठन :

2. यूआईडीआई की स्थापना नीचे दिए गए विवरण के अनुसार एक आरंभिक केन्द्रीय टीम के रूप में की जाएगी जिसमें 115 अधिकारी एवं कर्मचारी होंगे।

| पद | स्तर | पदों की संख्या |
|----------------------------|--------------------------|----------------|
| 1 | 2 | 3 |
| यूआईडीआई ऑथोरिटी ऑफ इंडिया | | |
| महानिदेशक एवं मिशन निदेशक | अपर सचिव, भारत सरकार | 1 |
| उप महानिदेशक (डीडीजी) | संयुक्त सचिव, भारत सरकार | 1 |
| सहायक महानिदेशक (एडीजी) | निदेशक, भारत सरकार | 1 |
| सहायक स्टाफ | | |
| निजी सचिव | निजी सचिव | 3 |
| चपरासी | चपरासी | 2 |
| डाइवर | डाइवर | 2 |
| कुल जन संसाधन | | 10 |

(121)

| 1 | 2 | 3 |
|--|--------------------------|-----|
| यूआईडीएआई की राज्य/संघ राज्य क्षेत्र इकाइयां | | |
| राज्य/संघ राज्य क्षेत्र आयुक्त | संयुक्त सचिव, भारत सरकार | 35 |
| | सहायक सचिव | |
| निजी सचिव | निजी सचिव | 35 |
| चपरासी | चपरासी | 35 |
| कुल जन संसाधन | | 105 |
| कुल योग | | 115 |

यूआईडीएआई की भूमिका एवं उत्तरदायित्व

3. यूआईडीएआई का उत्तरदायित्व होगा कि वह यूआईडी स्कीम के कार्यान्वयन के लिए योजना एवं नीतियां निर्धारित करे, यूआईडी डेटाबेस रखे एवं संचालित करे और यह प्रचलित आधार पर इसके अद्यतन एवं अनुरक्षण के लिए उत्तरदायी हो।

4. यूआईडी स्कीमों के कार्यान्वयन के लिए यह आवश्यक होगा कि अन्य बातों के साथ-साथ यूआईडीएआई द्वारा निम्नलिखित उत्तरदायित्वों का भी वहन किया जाए :-

- निवासियों का यूआईडी बनाना और उन्हें सौंपना।
- यूआईडी को नियमित आधार पर भागीदार डेटाबेस से जोड़ने के लिए तंत्र एवं प्रक्रिया निर्धारित करना।
- तंत्र को अद्यतन बनाने और प्रचलित आधार पर यूआईडी डेटाबेस के अनुरक्षण से संबंधित नीतियां एवं प्रशासनिक कार्यविधि की रूपरेखा तैयार करना।
- कार्यान्वयन भागीदारों और प्रयोक्ता एजेंसियों के साथ समन्वय/सम्पर्क स्थापित करना तथा संघर्ष समाधान प्रक्रिया निर्धारित करना।
- विभिन्न सेवाओं की पूर्ति के लिए यूआईडी के प्रयोग एवं उपयुक्तता को परिभाषित करना।
- यूआईडी अस्तित्व चक्र को सभी स्तरों पर संचालित करना एवं उसका प्रबंध करना।
- यूआईडी के क्रियान्वयन के लिए विशेषकर अनुमोदित समय सीमा के संदर्भ में चरणबद्ध दृष्टिकोण अपनाना।
- यूआईडी के साथ एनपीआर के परितुलन (अनुमोदित कार्यनीति के अनुसार) को सुनिश्चित करने के लिए आवश्यक कदम उठाना।
- अन्य अभिनामित एजेंसियों के साथ क्रासलिंग करत हुए इसके वैधकरण के अतिरिक्त भागीदार एजेंसियों के बीच लिंकेज स्थापित करने में क्षेत्र स्तर के संस्थानों जैसे कि पीआरआई (ज़) की लोवरेजिंग के लिए उपाय सुनिश्चित करना।
- यूआईडी के संबंध में जागरूकता व सम्प्रेषण की कार्यनीति तैयार करना तथा इसका उपयोग।
- नए भागीदार/प्रयोक्ता एजेंसियों की पहचान करना।

• एकत्र किए गए और डिजिटोक्त किए गए डेटा घटकों के मानकीकरण को सुनिश्चित करने के लिए डेटा बेस की शुरूआत करने वाली एजेंसियों को आवश्यक निर्देश जारी करना और यूआईडी तथा इसके भागीदार डेटाबेस के बीच परितुलन व परस्पर संबंध को संभव बनाना।

• हाइरिंग/प्रतिधारण/संसाधन जुटाव/विभिन्न कार्यों की आउटसोर्सिंग तथा यूआईडीएआई और यूआईडीएआई के अंतर्गत सभी राज्य यूनिटों की बजटिंग और आयोजना से संबंधित नीतियां व प्रशासनिक कार्य प्रणाली तैयार करना।

5. योजना आयोग यूआईडीएआई को लॉजिस्टिक्स, आयोजना व बजटोय सहायकता मुहैया कराने के लिए नोडल एजेंसी होगा। योजना आयोग केन्द्रीय स्तर पर शुरू में कार्यालय और आईटी अवसंरचना मुहैया कराएगा।

6. यूआईडीएआई में प्रतिनियुक्ति पर नियुक्त अधिकारियों को शहरी विकास विभाग के साधारण पूल से सरकारी आवास मुहैया कराए जाएंगे।

सुवास पाणि, सचिव

नई दिल्ली, दिनांक 31 दिसम्बर 2008

सं. ए-44011/1/2008-प्रशासन-1--आई.ई.एस. के एस.ए.जी. स्तर पर उनकी पदोन्नति के परिणामस्वरूप पेट्रोलियम और प्राकृतिक गैस मंत्रालय के पदभार ग्रहण करने हेतु श्रीमती अर्चना एस. माथुर, निदेशक को दिनांक 31 दिसम्बर, 2008 के अपराह से योजना आयोग से कार्यमुक्त किया जाता है।

अनिल मल्होत्रा, उप सचिव

सं. ए-44011/1/2008-प्रशासन-1--आई.ई.एस. के एस.ए.जी. स्तर पर उनकी पदोन्नति के परिणामस्वरूप पूर्वोत्तर क्षेत्र विकास मंत्रालय में पदभार ग्रहण करने हेतु, श्रीमती कीर्ती सक्सेना, निदेशक को दिनांक 31 दिसम्बर, 2008 के अपराह से योजना आयोग से कार्यमुक्त किया जाता है।

अनिल मल्होत्रा, उप सचिव

सं. ए-44011/1/2008-प्रशासन-1--आई.ई.एस. के एस.ए.जी. स्तर पर उनकी पदोन्नति के परिणामस्वरूप आर्थिक कार्य विभाग में पदभार ग्रहण करने हेतु, श्री अनिल बिसेन, निदेशक को दिनांक 31 दिसम्बर, 2008 के अपराह से योजना आयोग से कार्यमुक्त किया जाता है।

अनिल मल्होत्रा, उप सचिव

सं. ए-44011/1/2008-प्रशासन-1--आई.ई.एस. के एस.ए.जी. स्तर पर उनकी पदोन्नति के परिणामस्वरूप जनजातीय कार्य मंत्रालय में पदभार ग्रहण करने हेतु श्रीमती ऊर्वशी साध्वानी, निदेशक को दिनांक 31 दिसम्बर, 2008 के अपराह से योजना आयोग से कार्यमुक्त किया जाता है।

अनिल मल्होत्रा, उप सचिव

RAJYA SABHA SECRETARIAT

New Delhi-110001, the 2nd February 2009

No. RS/1078/Estt.(P).—On attaining the age of superannuation, Shrimati Prakash Munjal, Joint Director retired from service with effect from the afternoon of 31st January 2009.

C. B. RAJ, Director

PLANNING COMMISSION

New Delhi, the 28th January 2009

No. A-43011/02/2009-Admn.I.—In pursuance of Empowered Group of Ministers' fourth meeting, dated 4th November 2008, the Unique Identification Authority of India (UIDAI) is hereby constituted and notified as an attached office under aegis of Planning Commission with following terms of reference and initial core staff composition:—

Composition:

2. UIDAI shall be set up with an initial core team of 115 officials and staff as per details given below:—

| Post | Level | No. of Posts |
|-------------------------------------|-------------------------------------|--------------|
| UID Authority of India | | |
| Director General & Mission Director | Additional Secretary Govt. of India | 1 |
| Deputy Director General (DDG) | Joint Secretary, Govt. of India | 1 |
| Assistant Director General (ADG) | Director, Govt. of India | 1 |
| Support Staff | | |
| PS | PS | 3 |
| Peon | Peon | 2 |
| Driver | Driver | 2 |
| Total Manpower | | 10 |
| State/UT Units of UIDAI | | |
| State/UT UID Commissioner | Joint Secretary, Govt. of India | 35 |
| Support Staff | | |
| PS | PS | 35 |
| Peon | Peon | 35 |
| Total Manpower | | 105 |
| Grand Total | | 115 |

Role and Responsibilities of UIDAI

3. UIDAI shall have the responsibility to lay down plan and policies to implement UID Scheme, shall own and

operate UID database and be responsible for its updation and maintenance on an ongoing basis.

4. Implementation of UID scheme will entail, inter alia, following responsibilities being undertaken by UIDAI:—

- Generate and assign UID to residents
- Define mechanisms and processes for interlinking UID with partner databases on a continuous basis
- Frame policies and administrative procedures related to updation mechanism and maintenance of UID database on an ongoing basis
- Co-ordinate/liaise with implementation partners and user agencies as also define conflict resolution mechanism
- Define usage and applicability of UID for delivery of various services
- Operate and manage all stages of UID lifecycle
- Adopt phased approach for implementation of UID specially with reference to approved timelines
- Take necessary steps to ensure collation of NPR with UID (as per approved strategy)
- Ensure ways for leveraging field level institutions appropriately such as PRIs in establishing linkages across partner agencies as well as its validation while cross linking with other designated agencies
- Evolve strategy for awareness and communication of UID and its usage
- Identify new partner/user agencies
- Issue necessary instructions to agencies that undertake creation of databases, to ensure standardization of data elements that are collected and digitized and enable collation and correlation with UID and its partner databases
- Frame policies and administrative procedures related to hiring/retention/mobilization of resources, outsourcing of various tasks and budgeting & planning for UIDAI and all State units under UIDAI.

5. Planning Commission shall be the nodal agency for UIDAI for providing logistics, planning and budgetary support. Planning Commission would provide initial office and IT infrastructure at central level.

6. Government housing will be provided to officers of UIDAI appointed on deputation from general pool of Department of Urban Development.

Dr. SUBAS PANI, Secy.

New Delhi, the 31st December 2008

No. A-44011/1/2008-Admn.I.—Consequent on her promotion to SAG of IES Ms. Archana S. Mathur, Director

(TO BE PUBLISHED IN PART-I, SECTION-2 OF THE GAZETTE OF INDIA)

GOVERNMENT OF INDIA
PLANNING COMMISSIONYojana Bhawan, Sansad Marg,
New Delhi, 28th January, 2009NOTIFICATION

No. A-43011/02/2009-Admn.I: In pursuance of Empowered Group of Ministers' fourth meeting, dated 4th November 2008, the Unique Identification Authority of India (UIDAI) is hereby constituted and notified as an attached office under aegis of Planning Commission with following terms of reference and initial core staff composition:-

COMPOSITION:

2. UIDAI shall be set up with an initial core team of 115 officials and staff as per details given below:

| Post | Level | No. of Posts |
|-------------------------------------|-------------------------------------|--------------|
| UID Authority of India | | |
| Director General & Mission Director | Additional Secretary Govt. of India | 1 |
| Deputy Director General (DDG) | Joint Secretary, Govt. of India | 1 |
| Assistant Director General (ADG) | Director, Govt. of India | 1 |
| Support Staff | | |
| PS | PS | 3 |
| Peon | Peon | 2 |
| Driver | Driver | 2 |
| Total Manpower | | 10 |
| State /UT Units of UIDAI | | |
| State / UT UID Commissioner | Joint Secretary, Govt. of India | 35 |
| Support Staff | | |
| PS | PS | 35 |
| Peon | Peon | 35 |
| Total Manpower | | 105 |
| Grand Total | | 115 |

Role and Responsibilities of UIDAI

3 UIDAI shall have the responsibility to lay down plan and policies to implement UID Scheme, shall own and operate UID database and be responsible for its updation and maintenance on an ongoing basis.

4 Implementation of UID scheme will entail, *inter alia*, following responsibilities being undertaken by UIDAI:

- Generate and assign UID to residents
- Define mechanisms and processes for interlinking UID with partner databases on a continuous basis
- Frame policies and administrative procedures related to updation mechanism and maintenance of UID database on an ongoing basis
- Co-ordinate / liaise with implementation partners and user agencies as also define conflict resolution mechanism
- Define usage and applicability of UID for delivery of various services
- Operate and manage all stages of UID lifecycle
- Adopt phased approach for implementation of UID specially with reference to approved timelines
- Take necessary steps to ensure collation of NPR with UID (as per approved strategy)
- Ensure ways for leveraging field level institutions appropriately such as PRIs in establishing linkages across partner agencies as well as its validation while cross linking with other designated agencies
- Evolve strategy for awareness and communication of UID and its usage
- Identify new partner / user agencies
- Issue necessary instructions to agencies that undertake creation of databases, to ensure standardization of data elements that are collected and digitized and enable collation and correlation with UID and its partner databases
- Frame policies and administrative procedures related to hiring / retention / mobilization of resources, outsourcing of various tasks and budgeting & planning for UIDAI and all State units under UIDAI.

5. Planning Commission shall be the nodal agency for UIDAI for providing logistics, planning and budgetary support. Planning commission would provide initial office and IT infrastructure at central level.

45

180

6. Government housing will be provided to officers of UIDAI appointed on deputation from general pool of Department of Urban Development.

(Signature)
(Dr. Subas Pani) 28/11/0

Secretary to the Government of India

The General Manager
Govt. of India Press
Faridabad.

Copy to:

1. Secretary to the President, Rashtrapati Bhavan, New Delhi
2. Secretary to the Vice-President, Maulana Azad Road, New Delhi
3. Cabinet Secretary, Rashtrapati Bhavan, New Delhi
4. Principal Secretary to the Prime Minister, South Block, New Delhi
5. Private Secretary to the Deputy Chairman, Planning Commission
6. All Ministers/Departments of Govt. of India
7. Chief Secretaries of all States/Union Territories
8. Secretary General, Rajya Sabha Secretariat, New Delhi
9. Secretary General, Lok Sabha Secretariat, New Delhi
10. Pr. Adviser (Admn & PC)/AS & FA/Adviser (C & I)/Director (GA)/DS (Admn.)
11. Pay & Accounts Officer, Planning Commission
12. Drawing & Disbursing Officer, Planning Commission
13. Accounts -I Section, Planning Commission.

SECRET
4(4)/57/2010/CC-UIDAI
PLANNING COMMISSION
GOVERNMENT OF INDIA

116
181
ANNEXURE R-13 - 20

Annex II
(REFERENCE PARA GRAPH 1)

SECRET

MOST IMMEDIATE
Copy No. _____

No. 1/11/8/2009-Cab.
GOVERNMENT OF INDIA (BHARAT SARKAR)
CABINET SECRETARIAT (MANTRIMANDAL SACHIVALAYA)

New Delhi, the 22nd October, 2009

Subject: Constitution of the Cabinet Committee on Unique Identification Authority of India (UIDAI) related issues.

The undersigned is directed to say that it has been decided with the approval of the Prime Minister to constitute the Cabinet Committee on Unique Identification Authority of India related issues with the following composition :

Prime Minister,
Shri Pranab Mukherjee, Minister of Finance,
Shri Sharad Pawar, Minister of Agriculture and Minister of
Consumer Affairs, Food & Public Distribution,
Shri P. Chidambaram, Minister of Home Affairs,
Shri S.M. Krishna, Minister of External Affairs,
Shri M. Veerappa Moily, Minister of Law and Justice,
Shri A. Raja, Minister of Communications and Information Technology,
Shri Mallikarjun Kharge, Minister of Labour and Employment,
Shri Kapil Sibal, Minister of Human Resource Development,
Shri C.P. Joshi, Minister of Rural Development and
Minister of Panchayati Raj,
Kumari Selja, Minister of Housing and Urban Poverty
Alleviation and Minister of Tourism.

Special Invitees.

Shri Montek Singh Ahluwalia, Deputy Chairman, Planning Commission.
Shri Nandan Nilekani, Chairman, UIDAI.

2. The functions of the Committee would be as under :

- i) All issues relating to the Unique Identification Authority of India including its organization, plans, policies, programmes, schemes, funding and methodology to be adopted for achieving the objectives of that Authority.

3. All cases will be placed before the Cabinet Committee on Unique Identification Authority of India related issues after following the usual processes/procedures including appraisal of the cases by appropriate bodies, inter-ministerial consultations etc.

Dis - P-1

SECRET
4(4)/57/2010/CC-UIDAI
PLANNING COMMISSION
GOVERNMENT OF INDIA

117
182

SECRET
- 2 -

4. Necessary amendments in the Government of India (Transaction of Business) Rules, 1961, will be issued in due course.

(K.L. Sharma)
for Cabinet Secretary
Tele: 2301 5802

To
All Members of the Council of Ministers.

Copy forwarded for information to the Deputy Chairman and Members of the Planning Commission.

(K.L. Sharma)
for Cabinet Secretary

✓ Copy forwarded for information to Shri Nandan Nilekani, Chairman, Unique Identification Authority of India (UIDAI).

(K.L. Sharma)
for Cabinet Secretary

Copy forwarded for information to:-

Secretary to the President,
Secretary to the Vice-President.

(K.L. Sharma)
Director (Cabinet)

Copy forwarded for information to:-

National Security Adviser,
Principal Secretary to the Prime Minister,
All Secretaries to the Government of India.

(K.L. Sharma)
Director (Cabinet)

SECRET

ANV

118
183
ANNEXURE R-14

No. I-11011/40/2012-DCT
Government of India
Planning Commission
(DCT Division)

Yojana Bhawan, Sansad Marg,
New Delhi - 110 001.
Dated, the 26th December, 2012.

OFFICE MEMORANDUM

Subject : Direct Benefits Transfer (DBT) in Pilot Districts - Standardized Formats for Collection of Basic Data - Guidelines.

In supersession of (i) Circular dated 13th December, 2012 issued by the Department of Financial Services on Action Plan for Beneficiaries Registrations for Direct Cash Transfer (ii) Letter dated 12th December, 2012 from Director General, Unique Identification Authority of India addressed to Secretaries to the Government of India, (iii) Guidelines on Application Development for Aadhaar Enabled Direct Cash Transfer Draft-Version 2, dated 14th December, 2012 issued by Department of Electronics and IT, the following guidelines are being issued in respect of Standardized Formats for collection of basic data for entry of Aadhaar Numbers and bank accounts details of beneficiaries of 34 schemes in pilot districts identified for the first phase roll out of DBT scheduled to commence on 1st January, 2013.

2. The Direct Benefits Transfer (DBT) programme envisages a switch from the present electronic transfer to bank accounts of the beneficiary to transfer of benefits directly to Aadhaar seeded bank accounts of the beneficiaries for the identified 34 Schemes in 43 districts of 16 States/UT. List of these Schemes is at Annexure A.

3. Of the 34 Identified Schemes, 20 are Scholarship schemes (11 CS + 9 CSS) and the rest 8 (5 CS + 3 CSS) are non-scholarship schemes belonging to M/o WCD, Labour and Health. Six schemes are New Schemes.

4. As a first step, it will need to be ensured that all the intended beneficiaries under these schemes have or get an Aadhaar number before commencement of the DBT. It is a fact however, that the levels of Aadhaar enrollment as well as number of bank accounts for beneficiaries of these programmes vary from district to district.

5. Moreover, it is also likely that not all the identified Schemes are being implemented in all the identified districts. For example, schemes relating to scholarships to Tribals, Overseas Scholarships, minorities, child labour etc. may not have beneficiaries in all districts.

119
184

6. All Ministries would, therefore, be required to assess the scheme-wise, district wise exact number of beneficiaries. A format for collection of scheme-wise data is at Annexure-B.

7. In view of the foregoing, a Plan of Action to commence the rollout of the DBT scheme has to be finalized. The following actions must be completed before commencing DBT rollouts:

- (i) Beneficiary data base has to be digitized. The format for digitalization is at Annexure-C. This information would need to be compiled for each scheme only once.
- (ii) Aadhaar has to be "seeded" with beneficiary database. For this, necessary technical support will be provided by the NIC unit.
- (iii) Wherever beneficiaries do not have Aadhaar number, they will have to be enrolled for Aadhaar by the UIDAI Registrar.
- (iv) Wherever beneficiaries have bank accounts, it will need to be linked with Aadhaar number.
- (v) Wherever beneficiaries do not have bank accounts they will have to be opened, for which Aadhaar, if available, may be used as KYC, by the Bank. The new bank account will then be seeded with Aadhaar. In case Aadhaar is not available, banks will proceed with opening new bank account and Aadhaar will be seeded whenever it becomes available.
- (vi) An IEC campaign is to be initiated to inform the beneficiaries of the programme and to encourage enrolment in Aadhaar and opening bank account.
- ✓ (vii) Robust but easy to access grievance redressal systems must be put in place to mitigate unforeseen hardships, system failures etc. and to ensure there is no denial of service to beneficiaries without Aadhaar or bank accounts.

8. On its part, UIDAI will -

- (i) Ensure that the enrolment of more than 95% of the targeted beneficiaries of the identified schemes is quickly attained in the pilot districts.
- (ii) Will help the Central Ministries / State Governments / District Authorities with seeding of the beneficiaries list and their bank accounts with Aadhaar numbers.

9. In turn, the Department of Financial Services will ensure that the bank accounts of targeted beneficiaries under the identified schemes in the pilot districts are not only opened but are also seeded with Aadhaar.



Unique Identification Authority of India
Planning Commission,
Yojana Bhavan,
Sansad Marg,
New Delhi 110001

~~120~~
185

ANNEXURE R-15

Biometrics Design Standards For UID Applications

Version 1.0
December 2009

Prepared by: UIDAI Committee on Biometrics

121
180

CONTENTS

| | | |
|------|---|----|
| 1 | EXECUTIVE SUMMARY..... | 4 |
| 2 | INTRODUCTION..... | 7 |
| 3 | OBJECTIVE..... | 8 |
| 4 | SCOPE..... | 9 |
| 5 | TARGET AUDIENCE..... | 10 |
| 6 | NORMATIVE REFERENCE..... | 11 |
| 7 | STANDARDS..... | 12 |
| 8 | TAILORING OF FACE IMAGE STANDARDS..... | 13 |
| 8.1 | SECTION 7 DIGITAL/PHOTOGRAPHIC REQUIREMENTS..... | 13 |
| 8.2 | SECTION 7 IMAGE COMPRESSION ALGORITHM | 13 |
| 8.3 | FACE RECORD FORMAT | 13 |
| 9 | TAILORING OF FINGERPRINT IMAGE STANDARD | 15 |
| 9.1 | SECTION 7: IMAGE ACQUISITION REQUIREMENTS | 15 |
| 9.2 | SECTION 8 FINGER IMAGE RECORD FORMAT | 15 |
| 10 | TAILORING OF MINUTIAE FORMAT STANDARD..... | 17 |
| 10.1 | SECTION 7.4.1.3 IMPRESSION TYPE..... | 17 |
| 10.2 | SECTION 7.5 EXTENDED DATA | 17 |
| 11 | TAILORING OF IRIS STANDARDS..... | 18 |
| 11.1 | SECTION 7.4.2.2 KIND..... | 18 |
| 11.2 | SECTION 7.4.2.4 IMAGE DATA..... | 18 |
| 12 | BEST PRACTICES..... | 19 |
| 12.1 | FACE..... | 19 |
| 12.2 | FINGERPRINT..... | 20 |
| 12.3 | IRIS..... | 21 |
| 12.4 | BIOMETRICS ACCURACY..... | 21 |
| 13 | MEMBERS..... | 23 |
| 13.1 | BIOMETRICS COMMITTEE..... | 23 |
| 13.2 | FACE SUB-COMMITTEE | 23 |
| 13.3 | FINGERPRINT SUB-COMMITTEE..... | 23 |
| 13.4 | IRIS SUB-COMMITTEE..... | 23 |
| | ANNEXURE I. NOTIFICATION OF UIDAI CONSTITUTING THE COMMITTEE..... | 24 |
| | ANNEXURE II TECHNICAL DATA..... | 29 |
| | BIOMETRICS BASICS..... | 30 |
| | FACE..... | 30 |
| | FINGERPRINT..... | 30 |
| | IRIS..... | 30 |
| | FACE IMAGE BEST PRACTICES | 32 |
| | SUMMARY..... | 32 |
| | ENROLMENT..... | 32 |
| | AUTHENTICATION..... | 34 |
| | FINGERPRINT BEST PRACTICES..... | 35 |
| | SUMMARY..... | 35 |

122
187

| | |
|---|----|
| ENROLMENT..... | 36 |
| AUTHENTICATION..... | 37 |
| IRIS IMAGE BEST PRACTICES..... | 40 |
| SUMMARY..... | 40 |
| ENROLMENT..... | 41 |
| AUTHENTICATION..... | 43 |
| BIOMETRICS ACCURACY..... | 44 |
| STEP 1: ESTIMATING ACHIEVABLE ACCURACY..... | 44 |
| STEP 2: IMAGE QUALITY DIFFERENCE..... | 46 |
| STEP 3 COMPARISON & QUALITY ESTIMATES..... | 49 |
| CONCLUSIONS..... | 51 |
| FACE IDENTIFICATION..... | 52 |
| IRIS..... | 53 |
| FUSED ACCURACY..... | 53 |
| ISO DOCUMENTS..... | 55 |
| REFERENCES..... | 56 |

123
188

1 Executive Summary

The Unique Identification Authority of India (UIDAI) was set up by the Govt. of India on 28 January 2009. The purpose of the UIDAI is to issue Unique Identification numbers to all residents in the country. The Authority set up a Biometrics Standards Committee in order to frame biometrics standards for use by the UIDAI and its partners. The first deliverable of the Committee was to frame biometric standards based on existing national and international standards, with the consensus of various government stakeholders. The second deliverable was to recommend appropriate biometrics parameters to achieve the UIDAI's mandate. The second goal of the Committee encompasses best practices, expected accuracy, interoperability, conformity and performance in biometrics standards.

After reviewing international standards and current national recommendations, the Committee concluded that the ISO 19794 series of biometrics standards for fingerprints, face and iris set by the International Standards Organization are the most suitable. These standards are widely accepted, and best embody previous experiences of the US and Europe with biometrics. The standards framed for the UIDAI are accordingly, fully compliant with the respective ISO standards, and are given in Sections 7 through 11.

The Committee notes that Face is the most commonly captured biometric, and frequently used in manual checking. However, stand-alone, automatic face recognition does not provide a high level of accuracy, and can only be used to supplement a primary biometric modality. Fingerprinting, the oldest biometric technology, has the largest market share of all biometrics modalities globally. The fingerprint industry also has a variety of suppliers and a base of experienced professionals necessary to implement the unique identity management solution at the scale that India requires. Based on these factors, the Committee recognises that a fingerprints-based biometric system shall be at the core of the UIDAI's de-duplication efforts.

The Committee however, is also conscious of the fact that de-duplication of the magnitude required by the UIDAI has never been implemented in the world. In the global context, a de-duplication accuracy of 99% has been achieved so far, using good quality fingerprints against a database of up to fifty million. Two factors however, raise uncertainty about the accuracy that can be achieved through fingerprints. First, retaining efficacy while scaling the database size from fifty million to a billion has not been adequately analyzed. Second, fingerprint quality, the most important variable for determining de-duplication accuracy, has not been studied in depth in the Indian context.

The Committee therefore held extensive meetings and discussions with international experts and technology suppliers. A technical sub-group was also formed to collect Indian fingerprints and analyze quality. Over 250,000 fingerprint images from 25,000 persons were sourced from districts of Delhi, UP, Bihar and Orissa. Nearly all the images were from rural regions, and were collected by different agencies using different capture devices, and through different operational processes. The analysis reported in Section 12.4 and the associated Annexure show that the UIDAI could obtain fingerprint quality as good as seen in developed countries, provided that proper operational procedures are followed and good quality devices are used. On the other hand there is

127
189

data to suggest that quality and therefore the accuracy drops precipitously if attention is not given to operational processes.

The demographic data (non-biometric data) is also used for improving de-duplication processes. It reduces the amount of manual labor required to establish genuine duplicates from a possible list of duplicate matches.

Further, it has also been observed that Iris, which for a long period of time was under the proprietary domain, is emerging as an important biometric modality after fingerprint and face. The accuracy and speed of iris-based systems currently deployed is promising and may be feasible in large-scale de-duplication systems.

Finally, it is possible to combine multiple biometric modalities including multiple fingerprints to increase overall de-duplication accuracy.

Recommendations

Based on the above deliberations, the Committee makes the following principal recommendations:

1. The Committee expects that the UIDAI could achieve at least 95% de-duplication accuracy using moderately good fingerprint images for a database size of 1 billion. Empirical image quality data of Indian ground conditions clearly show that such accuracy is achievable. In the global context, a de-duplication accuracy of 99% has been demonstrated to be achievable using good quality fingerprints against a database of up to fifty million.
2. In order to capture moderately good fingerprint images, a few simple but critical techniques during enrolment should be consistently followed, failing which material reduction in accuracy would occur. Manual and automated monitoring should be utilized to ensure consistent use of good enrolment practices.
3. In view of the above, the Committee feels that the UIDAI should collect photograph and ten fingerprints as per ISO standards described in Sections 8, 9 and 10.
4. Biometrics data are national assets and must be preserved in their original quality. In other words, quality must not be compromised through lossy image compression during storage or transmission.
5. While 10 finger biometric and photographs can ensure de-duplication accuracy higher than 95% depending upon quality of data collection, there may be a need to improve the accuracy and also create higher confidence level in the de-duplication process. Iris biometric technology, as explained above, is an additional emerging technology for which the Committee has defined standards. It is possible to improve de-duplication accuracy by incorporating iris. Accuracy as high as 99% for iris has been achieved using Western data. However, in the absence of empirical Indian data, it is not possible for the Committee to precisely predict the improvement in the accuracy of de-duplication due to the fusion of fingerprint and iris scores. The UIDAI can consider the use of a third biometric in iris, if they feel it is required for the Unique ID project.
6. A scheme must be designed to reward enrolling agencies for the capture of good quality images.

125
190

7. Specific best practices indicated in Section 12 should be observed in order to ensure interoperability, vendor independence, conformance to standards and improved performance.
8. The UIDAI along with other stakeholders should establish center(s) for on-going biometrics research, and provide reference implementation of enrolment process software designed for Indian conditions.

2 Introduction

The UID Authority of India (UIDAI) has been setup by the Govt. of India with a mandate to issue a unique identification number to every resident in the country. The UIDAI proposes that it create a platform to first collect the identity details of residents, and subsequently perform identity authentication services that can be used by government and commercial service providers. A key requirement of the UID system is to minimize/eliminate duplicate identities in order to improve the efficacy of the service delivery.

The UIDAI has selected the biometrics feature set as the primary method to check for duplicate identity. In order to ensure that an individual is uniquely identified in an easy and cost-effective manner, it is necessary to ensure that the captured biometric information can be used to carry out de-duplication. Consequently, for government and commercial providers to authenticate the identity at the time of service delivery, it is necessary that biometric information capture and transmission are standardized across all partners and users of the UID system.

The Government of India has in the past set up a number of expert committees to establish standards for various e-governance applications in the areas of Biometrics, Personal Identification and location codification standards. These committees have worked out standards in their respective categories, which may be uniformly applied for various e-governance standards.

As the UIDAI proposes to use biometrics for de-duplication and verification/authentication, it becomes essential to review the applicability and sufficiency of these standards in UID applications. It may also be necessary to enhance or clarify these standards, and frame the methodology for the implementation of biometrics to ensure that they serve the specific requirements of the Authority.

127
192

4 Scope

- To develop biometric standards that will ensure the interoperability of devices, systems and processes used by various agencies that communicate with the UID system.
- To review the existing standards and, if required, modify/extend/enhance them so as to serve the specific requirements of the UIDAI.
- To specify design parameters of the standards that will be used for the UID system.
- To estimate the accuracy achievable using different biometric modalities in the Indian environment.
- To make recommendations to the UIDAI on the use of biometric modalities.

From the standpoint of the biometrics industry, the UID system is a civilian application of biometrics. Although the primary focus is the UID system, the Committee believes that the specifications should meet the needs of all civilian applications. The Committee considers forensic application requirements out of scope.

3 Objective

The UIDAI biometrics committee ("the Committee") was constituted to provide the UIDAI with direction on the biometrics standards, suggest best practices and recommend biometric modalities for the UID system (Annexure I).

The objective of these biometrics specifications is to ensure consistent good quality biometric images and reliable interoperability across biometric capture devices, capture software and UID service delivery.

The success of the Unique ID is solely based on its ability to detect and eliminate duplicate identities during the enrolment process. The primary method for detecting duplicates will be through the comparison of the biometric feature set, which requires consistent, high quality images. A good biometric implementation design that ensures consistent quality from a variety of biometric capture devices is therefore, essential.

The biometrics will be captured for authentication by government departments and commercial organizations at the time of service delivery. They will invariably use capture devices and biometric software vendors different from the devices and software used by UIDAI. Consequently, biometric standards are essential to ensure reliable interoperability at reasonable cost during the authentication phase.

The purpose of this document is to identify applicable standards and recommend best practices to the UIDAI to achieve its objective.

127
192

4 Scope

- To develop biometric standards that will ensure the interoperability of devices, systems and processes used by various agencies that communicate with the UID system.
- To review the existing standards and, if required, modify/extend/enhance them so as to serve the specific requirements of the UIDAI.
- To specify design parameters of the standards that will be used for the UID system.
- To estimate the accuracy achievable using different biometric modalities in the Indian environment.
- To make recommendations to the UIDAI on the use of biometric modalities.

From the standpoint of the biometrics industry, the UID system is a civilian application of biometrics. Although the primary focus is the UID system, the Committee believes that the specifications should meet the needs of all civilian applications. The Committee considers forensic application requirements out of scope.

129
194

5 Target Audience

Any person or organization involved in designing, testing or implementing UID or UID compatible systems for the central government, state government or commercial organizations.

Any vendors and integrators of biometric devices and software targeting UID system compatibility.

6 Normative Reference

The following reference documents are indispensable for the application of this document.

IAFIS-IC-0110 (V3), WSQ Gray-scale Fingerprint Image Compression Specification 1997

ISO/IEC 15444 (all parts), Information technology – JPEG 2000 image coding system

ISO/IEC 19785-1:2006, Common biometric exchange formats framework – Part 1: Data elements specifications

ISO/IEC 19794-2:2005, Biometric data interchange formats – Part 2: Finger minutiae data

ISO/IEC 19794-4:2005, Biometric data interchange formats – Part 4: Finger Image data

ISO/IEC 19794-5:2005, Biometric data interchange formats – Part 5: Face Image data

ISO/IEC 19794-6:2005, Biometric data interchange formats – Part 6: Iris Image data

ISO/IEC CD 19794-6.3, Biometric data interchange formats – Part 6: Iris Image data working group draft

MTR 04B0000022, (Mitre Technical Report), Margaret Lepley, Profile for 1000 Fingerprint compression, Version 1.1, April 2004. Available at

http://www.mitre.org/work/tech_papers/tech_papers_04/lepley_fingerprint/lepley_fingerprint.pdf

131
196

7 Standards

In the current IT world, as interoperability between devices and IT systems becomes a growing concern, the question is not whether to use standards but which standards to use. ANSI, INCITS, CEN, Oasis and ISO are just a few of the prominent agencies with published biometrics standards. After reviewing the charter of each body and current state of biometrics in India, the Committee selected the ISO standard. Within the ISO body of biometrics standards, the Committee will use data format standards. These standards are widely supported by vendors, and are used extensively. ISO data format standards also contain the maximum empirical information on usage, interoperability and conformance.

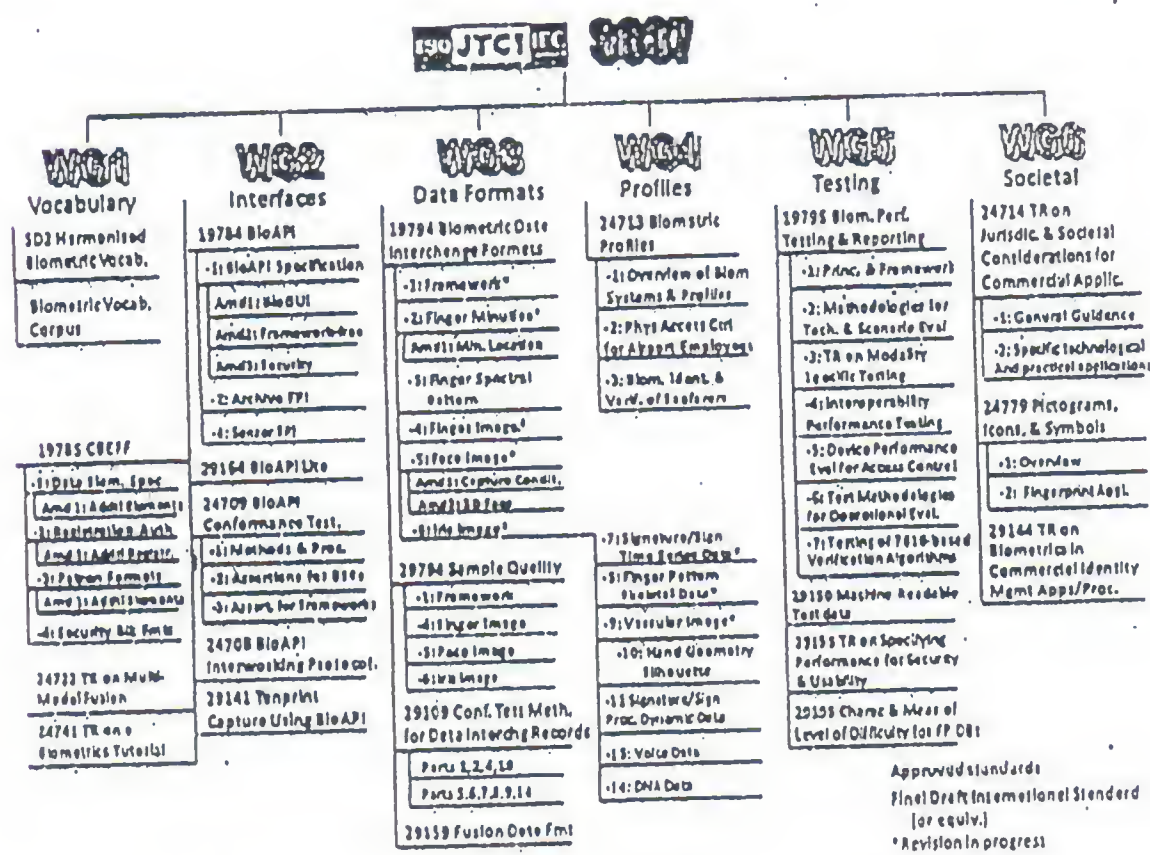


Figure 1 ISO Biometrics Standards Activity

132
197

8 Tailoring of Face Image Standards

The UIDAI Fingerprint Image Standard will adopt ISO/IEC 19794-5 Face Image Data Standard as the Indian Standard and will specify certain implementation values (tailoring) and best practices.

8.1 Section 7 Digital/Photographic requirements

The UIDAI will require face images for human visual inspection and duplicate check on a small subset. Visual inspection and automatic matching accuracy is directly related to the quality of the images. Therefore it is essential that the highest quality of images be consistently captured.

8.1.1 For Enrollment and Authentication

Defining the values for face image standards as shown in Section 7.2, table 2.

| Face Image Type Code | Scan resolution (dpi) | Color Space Code | Source Type Code | Inter-eye distance (pixels) | Facial Expression Code |
|----------------------|-----------------------|-------------------|------------------|-----------------------------|------------------------|
| Full Frontal (0x01) | 300 | 24 bit RGB (0x01) | 0x02 0x06 | 120 | 0x01 |

8.1.2 Source Type

Static face images (Code 0x02) from a digital still-image camera are strongly recommended. Single video frames from a digital video camera (Code 0x06) are also acceptable.

16.1.3 Expression

Face images should have neutral expression (non-smiling) with both eyes open and mouth closed.

16.1.4 Pose

Roll, pitch and yaw angle should not be more than $\pm 5^\circ$ (Figure 4 of ISO 19794-5).

8.2 Section 7 Image Compression Algorithm

8.2.1 For Enrolment

For enrolment, uncompressed images are strongly recommended. Lossless JPEG 2000 color compression will be accepted for legacy purposes only.

16.2.2 For Authentication

Code 0x01 - JPEG 2000 compression is recommended. Maximum compression ration is 10.

8.3 Face Record Format

8.3.1 CBEFF Header

The UIDAI will not use information defined in Section 5.3 of ISO document.

8.3.2 Facial Record Header

The UIDAI will maintain single facial image.

~~133~~
198

8.3.3 Facial Information Block

The UIDAI will not use information defined in Sections 5.5.1 to 5.5.6 of ISO document.

8.3.4 Feature Point Block

The UIDAI will not use geometric feature points defined in Section 5.6 of ISO document.

134
199

9 Tailoring of Fingerprint Image Standard

The UIDAI Fingerprint Image Standard will adopt ISO/IEC 19794-4 Fingerprint Image Data Standard as Indian Standard and specify certain implementation values (tailoring) and best practices.

9.1 Section 7: Image Acquisition Requirements

The duplicate check during the enrolment phase will use 1:N matching. 1:N matching for large gallery size and high enrolment rate will require substantial computing resources. The matching time and matching accuracy is directly related to the quality of the images. Therefore it is essential that the highest quality of images be consistently captured. It is also required that all ten fingers are captured whenever physically possible.

The goal during authentication is to achieve fast overall response while permitting a wide variety of capture devices and associated software. It is sufficient to capture only one or two fingers for reliable 1:1 authentication. The image quality needs for authentication are not as stringent as in enrolment.

9.1.1 For Enrolment

Setting level 31 or higher as shown in Section 7.1, table 1

| Setting level | Scan resolution (ppcm) | Scan resolution (dpi) | Pixel depth (bits) | Dynamic range (gray levels) | Certifications |
|---------------|------------------------|-----------------------|--------------------|-----------------------------|----------------|
| 31 | 197 | 500 | 8 | 200 | EFTS/F |

9.1.2 For Authentication

Setting level 28 or higher as shown in Section 7.1, table 2

| Setting level | Scan resolution (ppcm) | Scan resolution (dpi) | Pixel depth (bits) | Dynamic range (gray levels) | Certifications |
|-----------------|------------------------|-----------------------|--------------------|-----------------------------|----------------|
| 28 ¹ | 118 | 300 | 4 | 12 | UID |
| 30 | 197 | 500 | 8 | 80 | None |

9.2 Section 8 Finger Image record Format

9.2.1 Section 8.2.14 Image compression algorithm

9.2.1.1 Enrolment

Code 0 and 1 are strongly recommended. For legacy purposes only, lossless compression of code 2, 4 and 5 will be accepted.

9.2.1.2 Authentication

Code 4, compressed - JPEG 2000 is recommended. Code 0, 1, 2 and 5 are also acceptable. Code 3 must not be used. Maximum compression ration is 15.

¹ Level 28 is not specified in FBI's Electronic Fingerprint Transmission Specifications, Appendix F (commonly referred to as EFTS/F). It has been created to accommodate certain class of new generation lower cost single finger capture devices.

135
200

9.2.2 Section 8.3.3 Finger/palm position

The valid values for finger/palm position are 0 through 10, 13 through 15.

9.2.3 Section 8.3.7 Impression type

For enrolment image, only code 0 or 9 will be used. Authentication impression can be of type 0, 1, 8 or 9.

9.2.4 Section 8.3.10 Finger/palm image data

The estimated optimal fingerprint image captured under aforementioned specification of this standard in bitmap is 7.5MB per subject.

136
201

10 Tailoring of Minutiae Format Standard

UID Minutiae Format Standard will adopt the ISO/IEC 19794-2 Minutiae Format Standard as the Indian Standard and specify certain implementation values (tailoring) and best practices.

10.1 Section 7.4.1.3 Impression Type

For enrolment image, only code² 0 or 9 will be used. Authentication impression can be of type 0, 1, 8 or 9.

10.2 Section 7.5 Extended Data

While the extended data area allows for the inclusion of proprietary data within the minutiae format, this is not intended to allow for alternate representation of data that can be represented in open manner, as defined in ISO/IEC 19794-2. In particular, ridge count data, core and delta data or zonal quality information shall not be represented in proprietary manner to the exclusion of publicly defined data formats.

The UID authentication process will not utilize extended data area for verification.

² Codes specified in ISO/IEC 19794-4, Section 8.3.7 are newer and superset of this table. Hence the reference is made to ISO/IEC 19794-4 Table 7.

11 Tailoring of Iris Standards

UID Iris Image Standard will adopt the ISO/IEC 19794-6 Iris Image Data Standard as the Indian Standard and specify certain implementation values (tailoring) and best practices. The current (2005) version is under revision. A new version (2010) is expected to clear the ISO/IEC JTC 1/SC 37 sub-committee in January 2010. Therefore all references below are to the latest (November 2009) draft of the proposed standard. The Committee will revise this section after the ISO standard is published.

11.1 Section 7.4.2.2 Kind

Allowable values are KIND-VGA (2) and KIND_CROPPED (3) in Table 5.

11.2 Section 7.4.2.4 Image data

Every effort must be made by the vendor to register Capture Device Vendor ID and Capture Device Type ID with the appropriate registration authority. It is strongly recommended that these fields as described in Table 6 not be filled with zero value.

It is strongly recommended that quality information consisting of Quality score, Quality algorithm vendor ID and Quality algorithm ID as described in Table 6, shall be provided.

#39
203

12 Best Practices

Specific recommendations for each modality listed below are based on prevailing standards, best practices followed by international users and the ground reality in India.

12.1 Face

| Key Decisions | | Decision Type | Summary of Decisions |
|-----------------------|-------------------------------------|---------------|--|
| Enrolment | | | |
| | Image capture | R | Full frontal, 24 bit color |
| | Digital/Photographic requirements | R, S | Per ISO 19794-5 Section 7.3, 7.4, 8.3 and 8.4 with Section 8.3 of Technical Corrigendum 2. Inter-eye distance – minimum 120 pixels. |
| | Pose | S | Per ISO 19794-5 Section 7.2.2 |
| | Expression | R, S | Neutral expression. Specified as best practices. |
| | Illumination | S | Per ISO 19794-5 Section 7.2.7 |
| | Eye Glasses | S | Per ISO 19794-5 Section 7.2.11 |
| | Accessories | R | Permissible for medical and ethical reasons only. |
| | Multiple samples of face | M | Yes. Recommended for automatic face recognition. |
| | Operational | S | Per ISO 19794-5 Section 7.2.4 - 7.2.10 |
| | Assistance | R | Yes. Specified as best practices. |
| | Segmentation and feature extraction | M | Recommended for automatic face recognition |
| | Quality check | R | Yes. Specified as best practice. |
| | Storage & compression | S | Uncompressed image strongly recommended. For legacy reasons, lossless JPEG 2000 color accepted. |
| Authentication | | | |
| | Image capture | R | Same as enrollment |
| | Compression | S | JPEG 2000 color compression recommended. Compression ratio to be less than 10:1. |
| | Number of Images | R | One full frontal image |

Figure 2 Face Image

139
204

12.2 Fingerprint

| Key Decisions | | Decision Type ³ | Summary of Decisions |
|------------------------|-------------------------------|----------------------------|---|
| Enrolment | | | |
| Image capture | | | |
| | Plain or rolled | R | Plain, live scan |
| | Number of fingers | R | Ten |
| | Device characteristics | S | Setting level 31 or above, EFTS/F certified |
| | Quality check | R | Yes – specified as best practice |
| Operational | | | |
| | Assistance | R | Yes – Specified as best practice |
| | Corrective measure | R | Yes – Specified as best practice |
| Storage & transmission | | | |
| | Compression | S | Uncompressed images strongly recommended. For legacy reasons, lossless JPEG 2000 or WSQ compression accepted. |
| | Storage format | S | Per ISO Section 8.3. No deviation necessary |
| | Minutiae format | S | Per ISO 19794-2. No deviation necessary. |
| | Multi-finger fusion algorithm | R | Recommended. Application dependent. |
| Authentication | | | |
| Image capture | | | |
| | Number of fingers | R | No minimum, no maximum. Application dependent. Recommended as best practice |
| | Any finger option | M | Yes. Recommended as best practice |
| | Retry | R | Maximum 5. Recommended as best practice. |
| | Device characteristics | S | Setting level 28 or above |
| | Transmission format | S | Per ISO. No tailoring necessary |
| | Compression | S | JPEG 2000 compression recommended. Compression ratio to be less than 15:1 |
| | Minutiae format | S | Per ISO 19794-2. No tailoring necessary |

Figure 3 Fingerprint

³ R: Recommendation based on best practice/empirical data, S: Standard based, M: Management judgment.

140
205

12.3 Iris

| Decision | | Decision Type | Summary of Decision |
|----------------|------------------------|---------------|---|
| Enrolment | | | |
| | Image | R | Two eyes, > 140 pixel image diameter (170 pixel preferred), image margin 50% left and right, 25% top and bottom of iris diameter |
| | Device Characteristics | R | Tethered, autofocus, continuous image capture, exposure < 33 milli-second, distance >300 mm for operator control, > 100mm enrollee control |
| | Operational | M | Operator controlled strongly preferred. No direct natural or artificial light reflection in the eye, indoor. |
| | Segmentation | R | Non-linear segmentation algorithm |
| | Quality Assessment | R | Per IREX II recommendations ⁴ |
| | Compression & Storage | S | ISO 19794-6 (2010) data format standard as tailored in Section 11. JPEG 2000 or PNG lossless compression, KIND_VGA of Table A.1 of ISO 19794-6 (2010). |
| Authentication | | R, S | Same as enrollment except One or two eyes JPEG 2000 KIND_CROPPED of Table A.1 |

Figure 4 Iris

12.4 Biometrics Accuracy

The UIDAI's charter of assuring uniqueness across a population of 1.2 billion people mandates the biometrics goal of minimizing the False Accept Rate (FAR) within technological and economical constraints.

All published empirical data is reported using Western populations and database sizes of tens of millions. An accuracy rate (i.e., True Acceptance Rate) of 99% is reported in the test of commercial system performance[23]. Two factors however raise uncertainty on the extent of accuracy achievable through fingerprints: First, the scaling of database size from fifty million to a billion has not been adequately analyzed. Second, the fingerprint quality, the most important variable for determining accuracy, has not been studied in depth in the Indian context.

⁴ IREX II study conducted by NIST will be published in April 2010. It will provide definite empirical result of impact of image quality on matching accuracy and speed. For fingerprint the analogous study resulted in creation of NFIQ, NIST Fingerprint Image Quality algorithm. We anticipate similar outcome from IREX II. IREX II will be normative annexure to ISO 19794-6 (2010).

206

A technical sub-group was formed to collect Indian fingerprints and analyze quality. Over 250,000 fingerprint images from 25,000 persons were sourced from districts of Delhi, UP, Bihar and Orissa. Nearly all were from rural regions, collected by different agencies using different capture devices and through different operational processes. Analysis reported in Annexure showed the UIDAI could obtain as good fingerprint quality as seen in developed countries, provided that proper operational procedures are followed and good quality devices are used. On the other hand there is data to suggest that quality and therefore the accuracy drops precipitously if attention is not given to operational processes.

Based on rather extensive empirical results compiled by NIST and a first cut of Indian data analyzed in a short period, the following broad categorization can be made

1. The UIDAI can obtain fingerprint quality as good as that seen in developed countries. There is good evidence to suggest that fingerprint data from rural India may be as good as elsewhere when proper operational procedures are followed and good quality devices are used. There is also data to suggest that quality drops precipitously if attention is not given to operational processes.
2. It is possible to closely predict the expected fingerprint recognition performance. In the experiments, at 95% confidence, the sample database of a rural region is expected to achieve similar accuracy as Western data. By extrapolating NIST analysis of Western data, it is possible to conclude that fingerprint alone is sufficient to achieve minimum accuracy level of 95%, with moderately good fingerprints images.
3. Face is an invaluable biometric for manual verification. Its potential to contribute materially to improved FAR rate is however, limited particularly because of extremely large database size and high value of target accuracy.
4. Iris can provide accuracy comparable to fingerprint. Therefore fused score of two uncorrelated modalities will provide better accuracy than any single modality and could achieve the target accuracy.

Empirical data has highlighted several non-technical factors that can impact accuracy more significantly than technical accuracy improvement efforts.

- Simple operational quality assurance. A few simple operational techniques such as keeping a wet towel or maintaining the device in good working order can be superior to squeezing an additional fraction of a percent in accuracy rates through technical improvements. An unchecked operational process can increase the false acceptance rate to over 10%.
- In the data analyzed, 2% to 5% of subjects did not have biometric records. Missing biometrics is a license to commit fraud. It is believed that the failure is due to poorly designed processes. The enrolment process when examined, had loopholes which prevented it from detecting such omissions.
- The biometric software needs to be tuned to local data. Un-tuned software can generate additional errors in the range of 2 to 3%.

142
207

13 Members

13.1 Biometrics Committee

| | Name, Affiliation |
|-----|---|
| 1. | Dr. B. K. Gairola, DG NIC - Chairman |
| 2. | Dr. C. Chandramauli - Registrar General of India (RGI) - Member |
| 3. | Dr. D. S. Gangwar, Joint Secretary, Rural Development- Member |
| 4. | Dr. A. M. Pedgaonkar, RBI - Member |
| 5. | Mr. Pravir Vohra, ICICI - Member |
| 6. | Prof. Deepak Phatak, IIT Bombay - Member |
| 7. | Prof. Phalguni Gupta, IIT Kanpur - Member |
| 8. | Mr. R. S. Sharma, DG UIDAI - Member/Convener |
| 9. | Mr. Rajesh Mashruwala, UIDAI - Member |
| 10. | Mr. Srikanth Nadhamuni, UIDAI - Member |

13.2 Face Sub-committee

| | |
|----|-----------------------|
| 1. | Dr. Richa Singh |
| 2. | Dr. Mayank Vatsa |
| 3. | Mr. Rajesh Mashruwala |

13.3 Fingerprint Sub-committee

| | |
|----|-----------------------|
| 1. | Prof. Phalguni Gupta |
| 2. | Dr. A. M. Pedgaonkar |
| 3. | Mr. Rajesh Mashruwala |
| 4. | Dr. Mayank Vatsa |

13.4 Iris Sub-committee

| | |
|----|-----------------------|
| 1. | Prof. Phalguni Gupta |
| 2. | Dr. Mayank Vatsa |
| 3. | Mr. Rajesh Mashruwala |

143
208

Annexure I

Notification of UIDAI constituting the Committee

HAY
209

No. 45/DG-UIDAI/2009
Government of India
Planning Commission
Unique Identification Authority of India

R No. 321, Yojana Bhavan
New Delhi - 110 001

Dated: September 29, 2009

OFFICE MEMORANDUM

The UID Authority of India has been setup by the Govt. of India with a mandate to issue a unique identification number to all the residents in the country. The main objective is to improve benefits service delivery, especially to the poor and marginalised sections of the society. To deliver its mandate, the UID Authority proposes to create a platform to first collect the identity details and then to perform authentication that can be used by several govt. and private service providers. A key requirement of the UID system is to minimize/eliminate duplicate UIDs in order to improve the efficacy of the service delivery. A possible way to ensure uniqueness of IDs (so that one resident gets only one ID) is to use biometric technologies. In order to ensure that an individual is uniquely identified and authenticated in an easy and cost-effective manner, it is necessary to ensure that the biometric information which is captured is capable of carrying out the de-duplication at the time of collection of information. Further, in order to achieve interoperability it is important that the capture and use of biometric information is standardized across all the partners and users of the UID system.

The Government of India, in the past, had set up a number of expert committees for standards to be used for various e-governance applications in areas of Biometrics, Personal Identification and Location Codification Standards. These committees have worked out few standards in the respective categories to be uniformly applied for various e-governance standards.

As UIDAI proposes to use biometrics for de-duplication and verification/authentication, it becomes essential to review the applicability and sufficiency of these standards in UID applications, modify/extend/enhance them to ensure that they serve the specific requirements of UIDAI and frame the methodology for its implementation.

In view of the above, a Committee for framing the Biometric Standards for UIDAI is being setup to review the existing standards and modify/extend/enhance them so as to achieve the goals and purpose of UIDAI for de-duplications and authentication.

1. Charter of the Biometric Standards Committee

- To develop biometric standards that will ensure interoperability of devices, systems and processes used by various agencies that use the UID system.
- To review the existing standards of Biometric and, if required, modify/extend/enhance them so as to serve the specific requirements of UIDAI relating to de-duplication and Authentication.

2. Composition of the Biometric Standards Committee

Following will be the composition of the Biometric Standards Committee:

1. Dr. BK Gairola, Director General, National Informatics Centre - Chairman
2. Dr. C. Chandramauli - Registrar General of India - Member
3. Dr. DS Gangwar, Jt Secretary, Min of Rural Development - Member
4. Dr. AM Radgaonkar, Reserve Bank of India - Member
5. Mr. Pravin Vora, ICICI - Member
6. Dr. Deepak Phatak, IIT Bombay - Member
7. Dr. Phalguni Gupta, IIT Kanpur - Member
8. Two Representatives from Technology Team of UIDAI - Members
9. Director General, UIDAI or his Nominee - Member/Convenor

Unique Identification Authority of India (UIDAI) will service this Committee.

The Committee will be able to invite representatives from user organisations and other Technology Experts as Special Invitees to solicit their views and advice on various aspects on the issue.

3. Technical Committee and Working Groups

The committee can also set up sub-committees that focus on various aspects of biometric standards such as fingerprints, Iris and facial image and working groups for conducting/developing reference implementations/proof-of-concept (POC) studies, specific research, field testing etc. on an as-needed basis. The Committee may meet from time to time and draft the standard document based on the feedback of sub committees and working groups and submit recommendations. The Committee may also set its own review process before recommending the final standards.

146

21

Working Groups can be created to assist the above committees by conducting proof-of-concept (POC) studies, specific research, field testing etc.

4. Review process

It is important that the standards remain unbiased, pragmatic, vendor neutral, interoperable, and cost effective. In biometrics where technology continues to progress rapidly, three parties - vendors, academia and enterprise users - have great deal of knowledge of the technology. The Committee's review process will leverage their knowledge without compromising on its charter.

The technical committee will publish a draft version of the document and solicit structured feedback from the members of the committee, technology vendors, academia and enterprise users. Such review process will also provide sufficient advance notice to the vendors to begin upgrade to their solution, thus reducing lead time between the final standards adoption and conforming solutions.

The feedback from the various groups will be reviewed by the technical committee and suitable changes made in order to incorporate useful inputs. The final draft will be sent over for a final review and then the ratified version of the standards will be released.

5. Deliverables of the committee

- Obtain consensus from Government stakeholders to adopt and use a common set of standards for interoperability, containment of biometrics system cost and wide spread propagation of Biometrics in governmental and private sectors.
- Review the existing standards of Biometric and, if required, modify/extend/enhance them so as to serve the specific requirements of UIDAI relating to de-duplication and Authentication.
- Ratify Biometrics standards from applicable base Indian and International standards, which meet needs of the UIDAI.
- Recommendation to UIDAI users to assure interoperability of biometrics data.
- Develop certification criteria for conformity, interoperability and performance.
- Maintain & Publish registry of recommended biometrics standards, interoperability recommendations and certification criteria.

147
212

6. Time-Frame

Keeping in view the commitment of UIDAI to start issuing UIDs within twelve to eighteen months, it is necessary that the Committee presents its report on standards as early as possible. Hence the Committee will present its Final Report to the undersigned on Biometric Standards to be adopted by UIDAI within 90 days of its constitution.

7. Miscellaneous

The non-official members of the Committee and Special Invitees will be reimbursed the cost of their travel and other incidental expenses as per Rules as and when they travel to attend the Committee meetings.


28.9.09

(R. S. Sharma)
Director General & Mission Director

Copy forwarded to the Chairman and Members of the Committee for information and necessary action.

Copy to: Cabinet Secretary/ Principal Secretary to the PM/All Secretaries to Govt. of India/All Chief Secretaries of the States/UTs for information.

#78
213

Annexure II Technical Data

249
214

Biometrics Basics

Biometrics is the science of establishing the identity of an individual based on the physical, chemical or behavioural attributes of the person. The relevance of biometrics in modern society has been reinforced by the demand for large-scale identity management systems whose functionality relies on accurately determining an individual's identity. No single biometric is expected to effectively meet all the requirements imposed by all applications. In other words, no biometric is ideal, but a number of them are admissible[1].

Demographic data is used along with the biometric information to improve the de-duplication process. For example, when a duplicate is suspected, a manual review of all available information of the person will also include a review of the demographic data.

Face

Photos of the face are commonly used in various types of identification cards and there is wide public acceptance for this biometric identifier. Face recognition systems are the least intrusive type of biometric sampling system, requiring no contact or even awareness of the subject. The face biometric can work with legacy photographs, videotapes and other image sources.

A face needs to be well lighted using controlled light sources for automated face authentication systems to work well. There are many other such technical challenges associated with robust face recognition. Face is currently a poor biometric for use in de-duplication. It performs better in verification but not at the accuracy rates that are sometimes claimed. An obvious way for an undesirable person to avoid face identification is by the use of disguise, which will cause False Negatives in a screening application. In general, it is a good biometric identifier for small-scale verification applications.

Fingerprint

There is a long tradition in the use of fingerprints for identification. Fingerprints are easily sampled with low-cost fingerprint scanners. They can also be sampled by traditional low-tech means and then cheaply and easily converted into digital images. Fingerprints also lend themselves very well to forensic investigation.

There is a large variation in the quality of fingerprints within the population. The appearance of a person's fingerprint depends on age, dirt, and cuts and worn fingers, i.e., on the occupation and lifestyle of the person in general. Sampling of the fingerprint is through contact, i.e., pressing the finger against the platen of a fingerprint reader. As a result, there can be technical problems because of the contact nature of acquisition and problems related to the cleanliness of the finger and the platen. Additionally, there are people who may not have one or more fingers [5].

Fingerprint technology constitutes approximately half of the total biometrics market⁵.

Iris

The iris is the annular region of the eye, bounded by the pupil and sclera on either side. Iris is widely believed to be the most accurate biometric, especially when it comes to False Accept Rates. Therefore, the iris would be a good biometric for pure de-

⁵ IDC & Acuity Market Research Reports.

150
215

duplication applications. The iris sample acquisition is done without physical contact and without too much inconvenience to the person whose iris image is being acquired. Iris has no association with law enforcement and has not received negative press and may therefore be more readily accepted.

There are few legacy databases and not much legacy infrastructure for collection of the iris biometric. Large-scale deployment is consequently impeded by the lack of an installed base. This will make the upfront investment much higher. Since the iris is small, sampling the iris pattern requires a lot of user cooperation or the use of complex and expensive devices. The performance of iris authentication can be impaired by the use of spectacles or contact lenses. Also, some people may be missing one or both eyes while others may not have the motor control necessary to reliably enroll in an iris based system.

Until recently, iris code representation and matching was proprietary and patented. Iris is emerging as the third standard biometric identifier after expiration of patents and changes in vendor practices.

The gross false accept and false reject error rates associated with the fingerprint, face and iris modalities reported in literature are shown in Figure 5 [2].

| Biometric Identifier | Reference | FRR | FAR |
|----------------------|------------|-------|-------|
| Fingerprint | NIST FpVTE | 0.1% | 1% |
| Face | NIST FRVT | 10% | 1% |
| Voice | NIST 2004 | 5-10% | 2-5% |
| Iris | ITIRT | 0.99% | 0.94% |

Figure 5 FAR and FRR error rates

151
216

Face Image Best Practices

Summary

Face images will be used primarily for human visual inspection. However, automatic face recognition may be used as the secondary means of authentication/de-duplication. Figure 6 summarizes key decisions for face images.

| Key Decisions | | Decision Type | Summary of Decisions |
|-----------------------|-------------------------------------|---------------|---|
| Enrolment | | | |
| | Image capture | R | Full frontal, 24 bit color Inter-eye distance - minimum 120 pixels. |
| | Digital/Photographic requirements | R, S | Per ISO 19794-5 Section 7.3, 7.4, 8.3 and 8.4 with Section 8.3 of Technical Corrigendum 2. |
| | Pose | S | Per ISO 19794-5 Section 7.2.2 |
| | Expression | R, S | Neutral expression. Specified as best practices. |
| | Illumination | S | Per ISO 19794-5 Section 7.2.7 |
| | Eye Glasses | S | Per ISO 19794-5 Section 7.2.11 |
| | Accessories | R | Permissible for medical and ethical reasons only. |
| | Multiple samples of face | M | Yes. Recommended for automatic face recognition. |
| | Operational Assistance | S | Per ISO 19794-5 Section 7.2.4 - 7.2.10 |
| | Segmentation and feature extraction | R | Yes. Specified as best practices. |
| | Quality check | M | Recommended for automatic face recognition |
| | Storage & compression | R | Yes. Specified as best practice. |
| | | S | Uncompressed image strongly recommended. For legacy reasons, lossless JPEG 2000 color accepted. |
| Authentication | | | |
| | Image capture | R | Same as enrollment |
| | Compression | S | JPEG 2000 color compression recommended. Compression ratio to be less than 10:1. |
| | Number of Images | R | One full frontal image |

Figure 6 Face

Enrolment

Face image capture

Full frontal face image provides sufficient information for both human visual inspection (by operator) and automatic face recognition algorithms. In order to obtain a good quality image, 24-bit color image with minimum 90 pixels of inter-eye distance is required. The Committee recommends at least 120 pixels for optimum quality. The image should contain well-focused nose to ear and chin to crown region. In special circumstances, assistance may also be provided but in no case should the face or body part (hand, arms) of the assisting person or any object appear in the photograph.

152
217

Digital/Photographic requirements

In the typical enrolment setup, a computer will be connected to the biometrics devices to constitute the enrolment station. A tethered biometrics device provides several advantages over a stand-alone device. First, it allows the images to be associated with enrollee demographic data at the point of capture, thus reducing possible errors. In villages where power source may be difficult to obtain, it is simpler to supply power from the computer.

For capturing face image, it is simpler for the operator to adjust the camera instead of the enrollee to position himself/herself at the right distance or in the right posture. The capture device should use auto focus and auto-capture functions. The output image should not suffer from motion blur, over or under exposure, unnatural colored lighting, and radial distortion. Interlaced video frames are not allowed.

Pose

Face image should be full frontal with 0° of yaw, pitch and roll angles. However, in operational conditions, variation of $\pm 5^\circ$ is permissible.

Expression

Expression strongly affects the performance of automatic face recognition and also affects accurate visual inspection by humans. It is strongly recommended that the face should be captured with neutral (non-smiling) expression, teeth closed and both eyes open.

Illumination

Poor illumination has high impact on the performance of face recognition. It is difficult for human operators as well to analyze and recognize face images with poor illumination. Proper and equally distributed lighting mechanism should be used such that there are no shadows over the face, no shadows in eye sockets, and no hot spots.

Eye Glasses

Face images with and without eyeglasses may have an impact on face recognition. The impact is greater if the glasses automatically tint under illumination. If the person normally wears glasses, it is recommended that the photograph be taken with glasses. However, the glasses should be clear and transparent so that pupils and iris are visible. If the glasses are with tint, then direct and background lighting sources should be tuned accordingly.

Accessories

Use of accessories that cover any region of the face is strongly discouraged. However, accessories like eye patches are allowed due to medical reasons. Further, accessories like turban are also allowed due to ethical reasons.

Multiple samples of face

For visual inspection by humans, the single face image of a person is sufficient. However, for de-duplication and authentication of individuals who do not have fingerprints, automatic face recognition is recommended. To perform accurate authentication in such cases, capture of multiple face images is strongly recommended during enrolment. There should be three samples, out of which one should be frontal image with yaw, pitch and roll angle as 0° . The other two images should be left and right semi profile with yaw as $\pm 20^\circ$ to $\pm 30^\circ$, and the roll and pitch should be 0° .

Operational

Similar to fingerprints, the single most important factor in obtaining better image quality is the operational process. While there are many qualitative factors in designing good operational processes, operator training and assistance are important for yielding good quality images. Operators will be trained to obtain the best possible face images that satisfy requirements.

Segmentation and feature extraction

Segmentation and feature extraction are only required for automatic face recognition algorithms. The algorithms for both remain proprietary.

Quality check

Image quality is one of the most important factors for both human inspection and automatic face recognition algorithms. The quality assessment algorithm should encode parameters like illumination, pose, blur, noise, resolution, inter-eye distance, image height and width, and horizontal and vertical position of the face. The quality assessment algorithm should be used at the time of enrolment to determine the quality score of the captured face image and image is stored only if it meets a certain quality threshold.

Storage and Compression

According to Figures 12 and 13 of ISO face image standards, the performance of face recognition algorithms reduce significantly if the compression factor is greater than 10. Further, as mentioned previously, these are our national assets and should be captured and stored for long-term use. For preserving the quality of image, it is strongly recommended that uncompressed images should be stored in the database.

Authentication

The authentication process consists of steps similar to enrolment.

Image Capture

Image capture for 1:1 verification should also follow standards for enrolment as defined earlier in this Section.

Compression

For verification, images with JPEG 2000 compression ratio of 10 will suffice. As per ISO standards, the image size after compression should not be less than 11 KB.

Number of Images

For both manual and automatic authentication, a single full frontal face image is sufficient. The captured image should conform to the digital/photographic requirements and quality thresholds mentioned above in the enrolment section.

154
219

Fingerprint Best Practices

Summary

Figure 7 summarizes the key parameters for fingerprint. The Committee further classifies the decision into

1. Standards based (S): Do ISO or other standard bodies directly provide available choices?
 2. Recommendation based (R): Are there studies that provide sufficient evidence for us to make an informed decision?
 3. Management judgment (M): Management decision based on project context.
- The remaining section has a brief explanation of each decision.

| Key Decisions | | Decision Type | Summary of Decisions |
|-----------------------------------|-------------------------------|---------------|--|
| Enrolment | | | |
| Image capture | | | |
| | Plain or rolled | R | Plain, live scan |
| | Number of fingers | R | Ten |
| | Device characteristics | S | Setting level 31 or above, EFTS/F certified |
| | Quality check | R | Yes - specified as best practice. Avoid NFIQ quality 4 and 5 level fingerprints. |
| Operational | | | |
| | Assistance | R | Yes - Specified as best practice |
| | Corrective measure | R | Yes - Specified as best practice |
| Storage & transmission | | | |
| | Compression | S | Uncompressed image strongly recommended. For legacy reasons, lossless JPEG 2000 or WSQ compression accepted. |
| | Storage format | S | Per ISO Section 8.3. No deviation necessary |
| | Minutiae format | S | Per ISO 19794-2. No deviation necessary. |
| | Multi-finger fusion algorithm | R | Recommended. Application dependent. |
| Authentication | | | |
| Image capture | | | |
| | Number of fingers | R | No minimum, no maximum. Application dependent. Recommended as best practice |
| | Any finger option | M | Yes. Recommended as best practice |
| | Retry | R | Maximum 5. Recommended as best practice. |
| | Device characteristics | S | Setting level 28 or above |
| | Transmission format | S | Per ISO. No tailoring necessary |
| | Compression | S | JPEG 2000 compression recommended. Compression ratio to be less than 15:1 |
| | Minutiae format | S | Per ISO 19794-2. No tailoring necessary |

Figure 7 Fingerprint

Enrolment

The enrolment process can be broken down into image capture ("client") and de-duplication ("server") side components. The client side captures the image, performs local processing and storage. The server side receives the image, performs quality check and finally executes the computational intensive task of duplicate checking against the gallery.

Image capture

During image capture, the factors to consider are:

1. Type of image and number of fingers to capture
2. Device used for capturing the image
3. Immediate processing including segmentation of slap, sequencing of fingers, rotational correction and quality check of image
4. Storage when the images need to be stored

Plain or rolled

The rolled image, common in forensic applications, contains twice as much information as the plain image. The plain image is easier to capture. A slap capture device can capture up to four plain fingers in one scan. The rolled image in contrast, must be captured one finger at a time. Rolled images requires operator guiding the rolling of each finger. The operation difficulty in capturing rolled image rules out its use in the UID system.

Number of fingers

In general, every additional finger increases accuracy and improves matching speed. Quality of finger image among the fingers is correlated. Still, two poor quality finger images are better than one poor quality finger image. Considering the fingerprint quality of rural workers, the Committee recommends capturing prints of all ten fingers, the maximum possible.

Device characteristics

Device characteristics cover scan resolution, pixel depth and dynamic range. A higher resolution device does not necessarily produce better images⁶. The biometrics sample captured during enrolment needs to be the best sample possible. Therefore following best practices of leading countries, the Committee recommends the use of EFTS/F certified devices that operate at level 31 or above.

Capture & quality check

Once the image has been captured, one can perform basic quality check and image improvement. The enrollee must be asked to retry enrolling if the image quality is poor. The algorithm can assign image quality score. The quality threshold score is an important decision. Images captured with a NIST Fingerprint Image Quality (NFIQ) value of 4 or 5 normally should not be used for enrolment purposes.

⁶ It should be noted that two devices with identical scan resolution, pixel depth and dynamic range do not provide similar quality images. A number of laboratory tests have shown that a 500 dpi device from one vendor performs better than a 1000 dpi device of another vendor. Nevertheless, these attributes are the only transparent way to specify the minimum device requirements.

156
221

Operational

The single most important factor in obtaining better image quality is the operational process. While there are many qualitative factors in designing good operational processes, the following have been shown to be critical factors:

1. Operator Assistance: Operators will be trained to guide the enrollee's hand and apply pressure if necessary to obtain best possible image quality.
2. Corrective measures & retries: If the initial capture is unsatisfactory, the operator will be trained to provide corrective measures such as wiping fingers with a wet cloth or applying lotion. Only after all such measures are exhausted in five attempts, will the operator be able to override the (forced capture) quality gate.

Storage and Transmission

Once the quality check is complete, the image needs to be retained. The data format of storage should be such that other applications can access the data.

Compression

Biometric data are national assets and should be captured and stored for long-term use. To preserve the quality, the Committee strongly recommends uncompressed images. Transmission of images may be made in JPEG 2000 or WSQ lossless compression for legacy or compatibility purposes. Any form of lossy compression is not accepted. In uncompressed mode, the total storage required for the entire population is 10,000 TB.

Storage format

ISO standard prescribed format is sufficient for our needs.

De-duplication minutiae format

The minutiae representation has been standardized. However, the standardization allows vendor proprietary data fields. The trade-off is between performance and accuracy through enhanced minutiae data versus higher level of vendor dependence. Based on the accuracy and performance trade-offs reported by NIST, it is acceptable to use the proprietary format of the extractor-matcher of the vendor selected for de-duplication.

Multi-finger fusion

Different algorithms are available to obtain consolidated score [7] and [28]. The selection of the algorithm will make material difference to the overall accuracy. ISO and other bodies do not make recommendations, nor do they provide empirical study. The UIDAI will conduct its own analysis to identify the best multi-finger fusion algorithm.

Authentication

The authentication process consists of steps similar to the enrolment process, but its requirements for accuracy, performance and interoperability are different. Since the authentication process is performing 1:1 verification, the captured image may be of lower quality compared to the image captured during the enrolment process.

157
222

Image capture

Number of fingers

It is obvious that a fewer number of fingers should be required for verification to achieve a satisfactory accuracy target. A single finger will be sufficient to provide the minimum standard of accuracy requirements. Applications requiring higher levels of accuracy may need additional fingers.

Any finger option

The normal practice is to use one specific finger, say the index finger for verification. However, current technology could allow the person to scan any finger. This is not merely a question of convenience. Certain fingers, depending on the condition of the finger, will perform better in matching. While one cannot easily determine this a priori, any frequent user will learn it by experience. This improves subsequent user experience and could potentially improve match accuracy.

Retry

The decision on number of retries has different implications during authentication. In case of enrolment, the final decision is to take the "best possible" image. The operator can thus "force capture". In case of authentication, the operator needs to find an alternate method of authentication if fingerprint verification fails. The operator/application would not know the cause of verification failure. The failure could be because the fingerprint did not match or image capture did not produce sufficient quality image for matching. In both cases, the match score is low enough for the system to declare "no match". A timeout will be implemented in service after five attempts.

Device characteristics

Device characteristics cover scan resolution, pixel depth and dynamic range. Higher resolution does not necessarily produce better images. Considering the UIDAI's goal of making authentication ubiquitous and the availability of low cost new technology devices, the Committee has defined a new standard for the scanner used in the authentication process. It is envisioned that the UIDAI will provide certification criteria for this standard.

Transmission format

The captured image needs to be sent to the UID server for matching in real time. Two factors will decide the format of the image to be sent. If the transmission bandwidth is low, it is prudent to send as little data as possible. On the other hand if the computing device associated with the capture device has very limited processing power, it is prudent to do minimal amount of local computation. In the first case, the transmission will contain extracted minutiae. In the second, it will contain the compressed raw image. For example, a capture device connected to a computer communicating over a mobile network could send minutiae by performing local extraction. A dedicated image capture device with built-in network connectivity is able to do little local processing and may send raw image.

The UID software will support raw image format, compressed image format as well as ISO standard minutiae format to be transmitted, in order to provide maximum flexibility during authentication. It is understood that raw or compressed image will give a higher level of accuracy.

158
223

Compression

If the raw image is to be sent, JPEG 2000 compression is recommended, WSQ compression may be acceptable for legacy purposes. A compression of up to 15 is acceptable. While uncompressed image will be accepted, it is not recommended. JPEG compression is not accepted. There is sufficient data to indicate that compression ratio of 15 does not affect verification accuracy. Compression is not relevant if minutiae data is to be sent for verification.

Minutiae format

As discussed in the previous section, the biometric sample being transmitted could be minutiae data or image. If the data is minutiae and the UID server has matcher that best pairs with the extractor used by the authenticating agency, it will use the proprietary data. If the server does not have matching matcher, it will only use "standard" minutiae data.

159
224

Iris Image Best Practices

Summary

Compared to fingerprinting, iris capture is less studied and less standardized. For example, fingerprint scanners are tested and certified per EFTS/F standard. No such equivalent iris device certification is available. It is necessary to provide greater number of parameter specifications to ensure quality iris capture.

Figure 8 summarizes key decisions for UIDAI iris design.

| Decision | | Decision Type | Summary of Decision |
|----------------|------------------------|---------------|---|
| Enrolment | | | |
| | Image | R | Two eyes, > 140 pixel image diameter (170 pixel preferred), image margin 50% left and right, 25% top and bottom of iris diameter |
| | Device Characteristics | R | Tethered, autofocus, continuous image capture, exposure < 33 milli-second, distance >300 mm for operator control, > 100mm enrollee control |
| | Operational | M, R | Operator controlled strongly preferred. No direct natural or artificial light reflection in the eye, capture location: indoor. |
| | Quality Assessment | R | Per IREX II recommendations ⁷ |
| | Compression & Storage | S | ISO 19794-6 (2010) data format standard as tailored in Section 11. JPEG 2000 or PNG lossless compression, KIND_VGA of Table A.1 of ISO 19794-6 (2010). |
| Authentication | | R, S | Same as enrollment except One and/or two eyes JPEG 2000 KIND_CROPPED of Table A.1 |

Figure 8 Iris

The remaining section has a brief explanation of each decision.

⁷ IREX II study conducted by NIST will be published in April 2010. It will provide definite empirical result of impact of image quality on matching accuracy and speed. For fingerprint the analogous study resulted in creation of NFIQ, NIST Fingerprint Image Quality algorithm. IREX II will be a normative annexure to ISO 19794-6 (2010).

260
225

Enrolment

Iris Image

Capture of two eyes simultaneously provides several advantages⁸. Iris pattern of each eye is not correlated, giving two independent biometric feature sets. It assures correct assignment of left and right eyes and allows for more accurate estimation of roll angle.

In order to obtain good quality template, the iris image diameter should be minimum 140 native pixels. The Committee recommends 170 pixels for optimum quality.

In order to retain sufficient image surrounding of the iris for the purpose of identifying the left or right eye as well as for a more accurate iris segmentation, the margins around the iris portion of the image need to be at least 50% of the iris diameter on the left and right sides of the image, and a least 25% of the iris diameter on the top and bottom of the image.

Device Characteristics

In the typical enrolment setup, a computer will be connected to the biometrics devices to constitute the enrolment station. A tethered biometrics device provides several advantages over a stand-alone device. First, it allows the images to be associated with the enrollee demographic data at the point of capture, thus reducing possible errors. In villages where a power source may be difficult to obtain, it is simpler to supply power from the computer.

Iris capture is a new experience for the public[34]. It is faster and simpler for the operator to adjust the camera instead of the enrollee positioning himself/herself at the right distance or in the right posture. It is recommended that the capture device should be more than 300 mm away from the enrollee to be considered non-intrusive. The capture device should use auto focus and auto-capture functions. In special circumstances where the enrollee has to position himself or herself, the capture device should be more than 100mm away but the device should use a visor or other mechanical alignment aid to enable the enrollee to position themselves.

In order to provide an acceptable level of usability and ease of alignment, the camera must allow for some variability in the position of the iris center relative to the camera. This variability is defined by position tolerances in the horizontal, vertical, and axial dimensions that together define a volume (the "capture volume") within which the center of the iris must be located in order to enable image capture. For two eye capture devices, the capture volume dimensions for devices without mechanical alignment aids are 19 mm wide, 14 mm high, and 20 mm deep, and for devices with such aids, 19 mm wide, 14 mm high, and 12 mm deep.

The ability of an iris image capture device to suppress motion blur and to freeze motion, is a function of exposure time. The maximum allowable value for the exposure time is less than 33 ms, recommended being 15ms.

The iris image capture device must be capable of capturing light in the range of 700 to 900 nanometers. The camera's near infrared illuminator(s) must have a controlled spectral content, such that the overall spectral imaging sensitivity, including the sensor characteristics, transfers at least 35% of the power per any 100 nm-wide sub-band of the 700 to 900 nm range.

⁸ Material derived from [32]

#61
226

The iris image capture sensor shall use progressive scanning.

In order to achieve acceptable time-to-capture and FTA rates, the iris image sampling frequency must be at least 5 frames per second.

The capture devices typically provide infrared lighting using LEDs to illuminate the iris. The illumination is in a range partly visible to the human eye. Illumination shall be compliant with illumination standard IEC 825-1 and safety specification ISO 60825-1.

In order to achieve acceptable recognition accuracy, the iris acquisition sensor must achieve a signal-to-noise ratio of at least 36dB.

Within the frequency range of interest, 700 to 900 nm, the iris sensor shall generate images with at least 8 bits per pixel.

Operational considerations

As mentioned earlier, it is strongly recommended that the operator and not the enrollee handle the capture device. The enrollee will be required to sit (or stand) in a fixed position, like taking a portrait photograph; the operator will adjust the camera.

The iris capture device or the connected computer shall be able to measure the iris image quality. The best practice recommendation is that an initial image quality assessment should be done to provide feedback to the operator during the capture process. The device should alert the operator if the captured iris image is of insufficient quality.

The iris capture process is sensitive to ambient light. No direct or artificial light should directly reflect off enrollee's eyes.

Segmentation and feature extraction

Segmentation and feature extraction remain proprietary. As reported in the IREX study, the vendor providing segmentation does not have to be the vendor providing matching algorithm. In fact, best of breed selection appear to be superior to any single-vendor solution.

Quality assessment

It has been noted that image quality is the single most important factor for match accuracy. IREX II study is underway to quantify and provide best practices recommendations on the image quality. The report, expected in April 2010, will become the normative annexure to ISO 19794-6 (2010). Therefore the Committee will defer detailed quality recommendations until publication of the standard.

One method widely used for ensuring good iris images is recommended here. An iris camera takes streaming images. It is recommended that the device take successive 3 to 7 images and use local matching algorithm to match them against each other (after feature extraction). The image is considered to be of satisfactory quality if hamming distance of the match is below 0.1.

Compression and storage

The iris images, like fingerprints are considered to be national assets. They should be stored in ISO standard format using either JPEG 2000 or PNG lossless compression (KIND_VGA). It is expected that each enrollee will require 150 Kbytes of storage space, thus requiring total storage space of 200 Terabytes for the entire population.

#162
227

Authentication

For 1:1 verification, any one eye will suffice, though application may require higher-level assurance whereby both eyes can be verified. Iris verification requires the image to be sent to the server for matching. It is recommended that the image be compressed to KIND_CROPPED_AND_MASKED or KIND_CROPPED using JPEG 2000. Resulting image size will be between 2KB to 10 KB. Any of the larger formats specified by the ISO standard are acceptable, though not necessary.

163
228

Biometrics Accuracy

The consequences of FAR and FRR during authentication are central to the judicial design of the UID system. FAR determines potential number of duplicates, FRR determines number of enrolments necessitating manual check, hence labor cost. While trade-off between the two rates is certainly possible, there are upper bound requirements for each. Upper bound for each rate is set at 1%.

No empirical study is available to estimate the accuracy achievable for fingerprint under Indian conditions. Indian conditions are unique in two ways:

- Larger percentage of population is employed in manual labor, which normally produces poorer biometric samples.
- Biometric capture process in rural and mobile environment is less controllable compared to the environmental conditions in which Western data is collected.

To estimate achievable accuracy under Indian conditions, following methodology was employed:

1. Estimate achievable accuracy under Western conditions for a one billion sized database.
2. Estimate difference in image quality between Western and Indian conditions.
3. Using image quality, estimate change in achievable accuracy under Indian conditions.

There is no indication to believe that iris accuracy changes from one racial/geographical population to another. However, no definitive study is available.

Step 1: Estimating achievable accuracy

NIST reports FAR of 0.07% at FRR 4.4% for 6 million fingerprint gallery size using two plain fingers [21]. Similar results were reported for FBI's IAFIS System of 46M samples. It is safe to conclude that 99% accuracy (TAR) can be achieved for database size of 50 million.

| Shape Filter | Thresholds 1300, 1880 | | Thresholds 1400, 2025 | | Matches per Second |
|--------------|--------------------------|-------|--------------------------|-------|--------------------|
| | FAR | TAR | FAR | TAR | |
| Off | 0.30% | 96.3% | 0.07% | 95.6% | 734K |
| On | 0.32% | 96.1% | 0.07% | 95.5% | 1035K |

Figure 9 Two-finger identification accuracy

Several NIST reports allow us to estimate the scaling of above data for larger gallery size and for ten fingers.

- False Acceptance Rate is linearly proportional to gallery size at constant TAR as shown in Figure 11.
- False Rejection Rate does not vary over gallery size as shown in Figure 12.
- Based on these findings, one can expect that on a database size that is 200 times larger (1.2 billion versus 6 million), the same system will have an FAR of

164
229

approximately $0.07 \times 200 = 14\%$. The FRR can be expected to be about 4% based on matching of 2 finger plain fingerprints.

- Figure 10 lists effect on FAR by increasing the number of fingers for the same FRR [22].

| Number of Fingers | FRR % | FAR % |
|-------------------|-------|-------|
| 2 | 10.3 | 29.2 |
| 10 | 10.9 | 0.0 |

Figure 10 Accuracy of multiple fingers

- Based on the above and reviewing underlying data, one can ballpark a 1,000 improvement in FAR between two-finger matching and ten-finger matching (all other things being equal). So the estimated FAR estimate of 14% should be expected to be 1,000 times less, that is, to 0.14% at FRR rate of 4%. Using further conversation factor of 10X change in FAR results in 2X change in FRR, this number is the equivalent of FAR 1.4% at FRR rate of 2%. In other words, NIST data indicates de-duplication accuracy (TAR) greater than 95% is achievable for ten-finger matching against a database size of one billion.

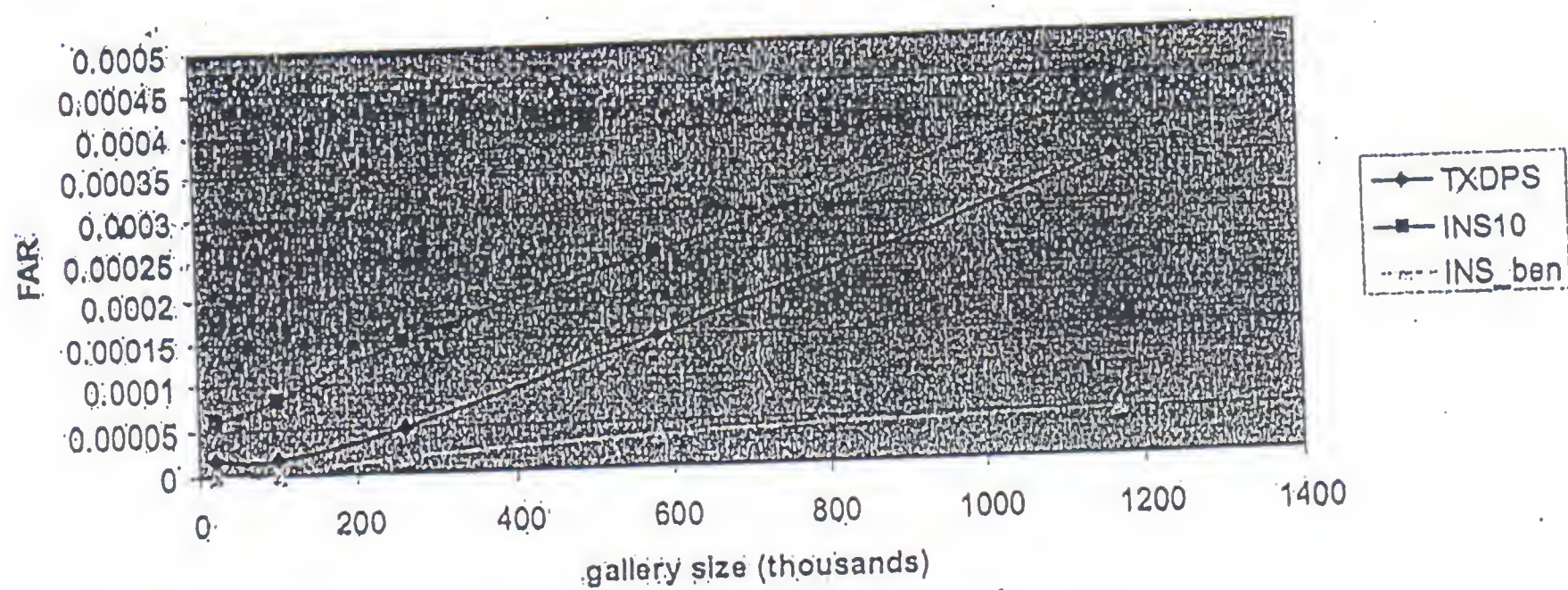


Figure 11 FAR as function of gallery size

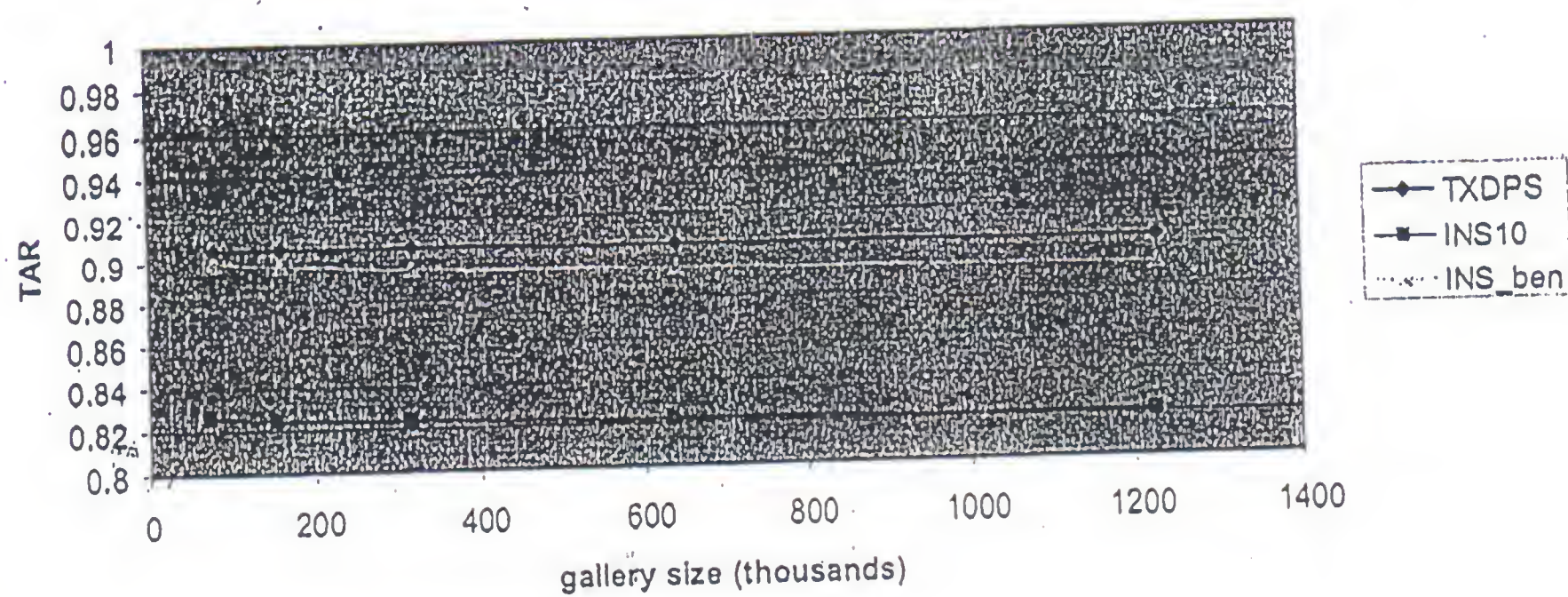


Figure 12 TAR as function of gallery size

465
230

Step 2: Image quality difference

It has been shown that match rates accuracy can be estimated from the fingerprint image quality score. NIST classifies scores into five bins. Western data accuracy rates for the bins are shown in Figure 13. Bins 1 and 2 are nearly identical, producing close to 99% true match in 1:1 verification. Bins 4 and 5 result in unacceptably low true match rates. Of particular note is bin 5, which could result in as low as 80% match rate (or 20% false accept rate).

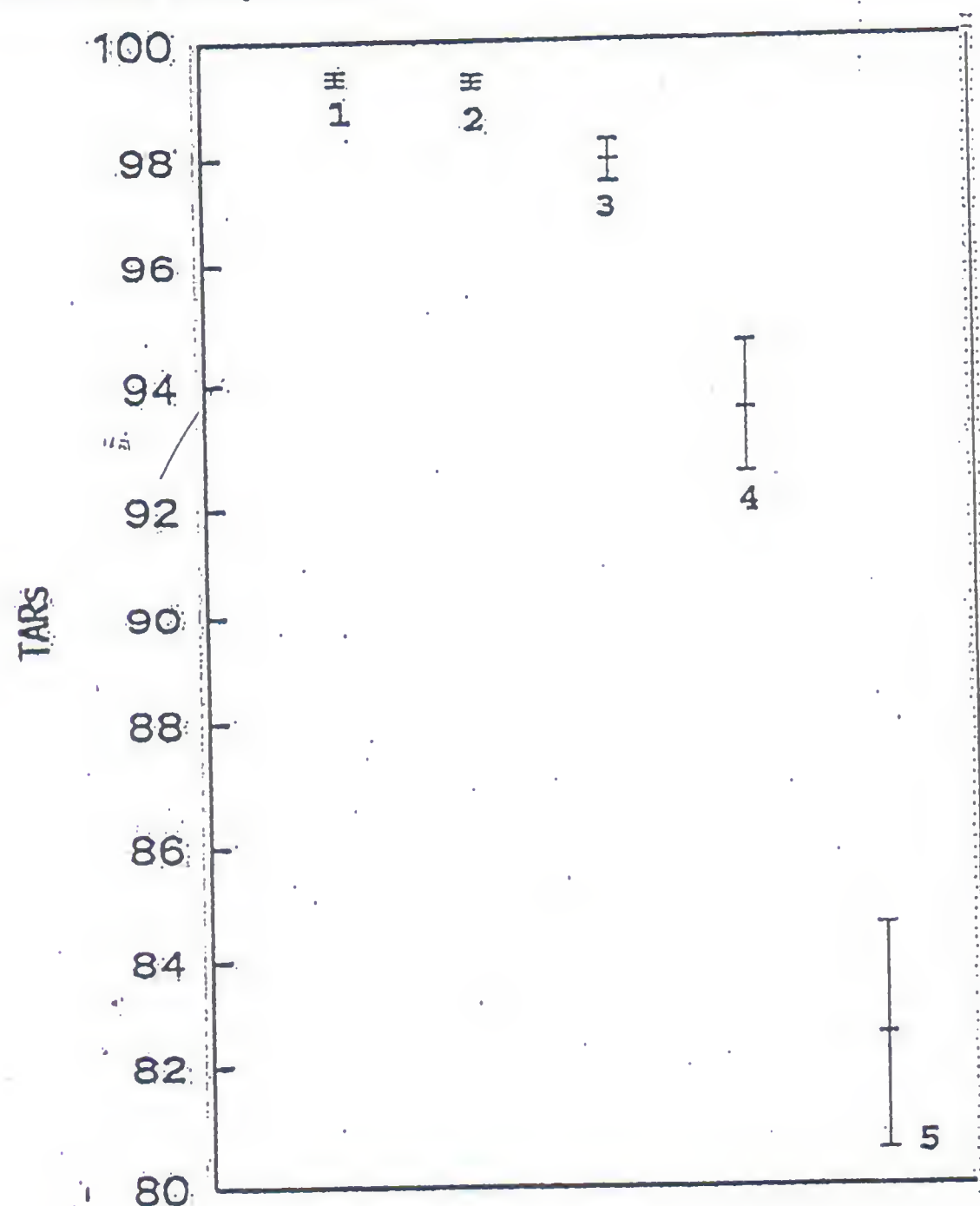


Figure 13 Accuracy Range by image quality

In a "typical" sample analyzed to arrive at the above rate[24], NIST has bin distribution shown in Figure 14 and Figure 15. Bins 4 and 5 in both datasets are less than 5% of the total sample.

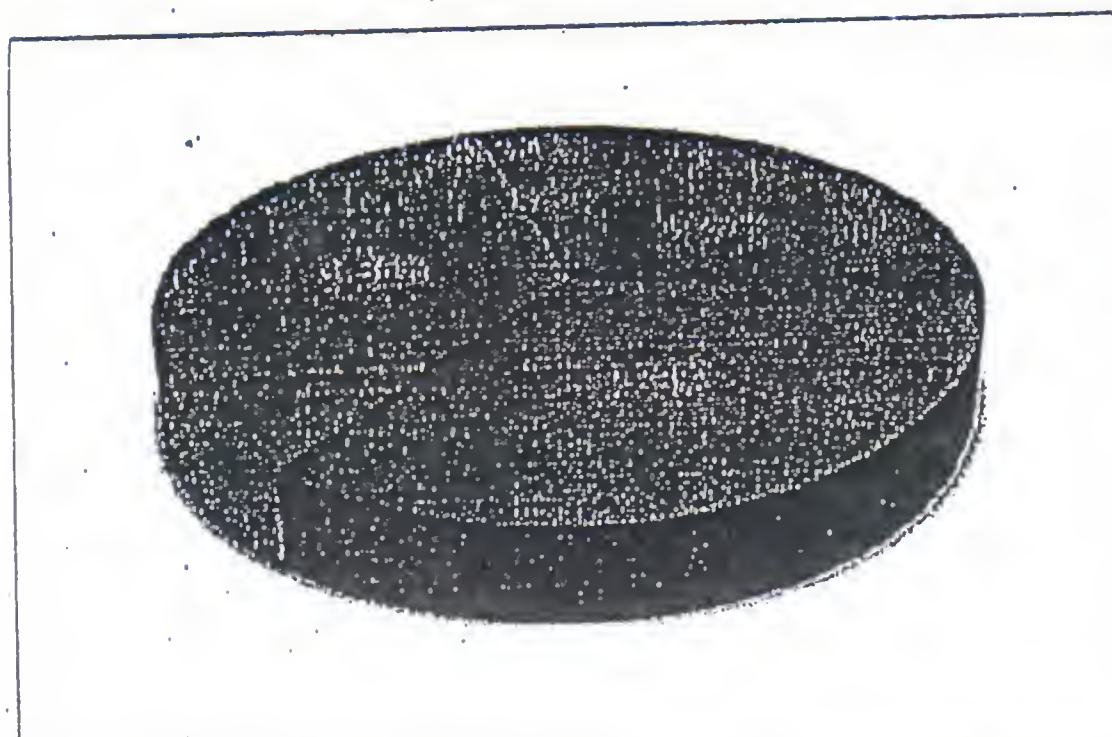


Figure 14 US-VISIT image quality distribution for right index finger

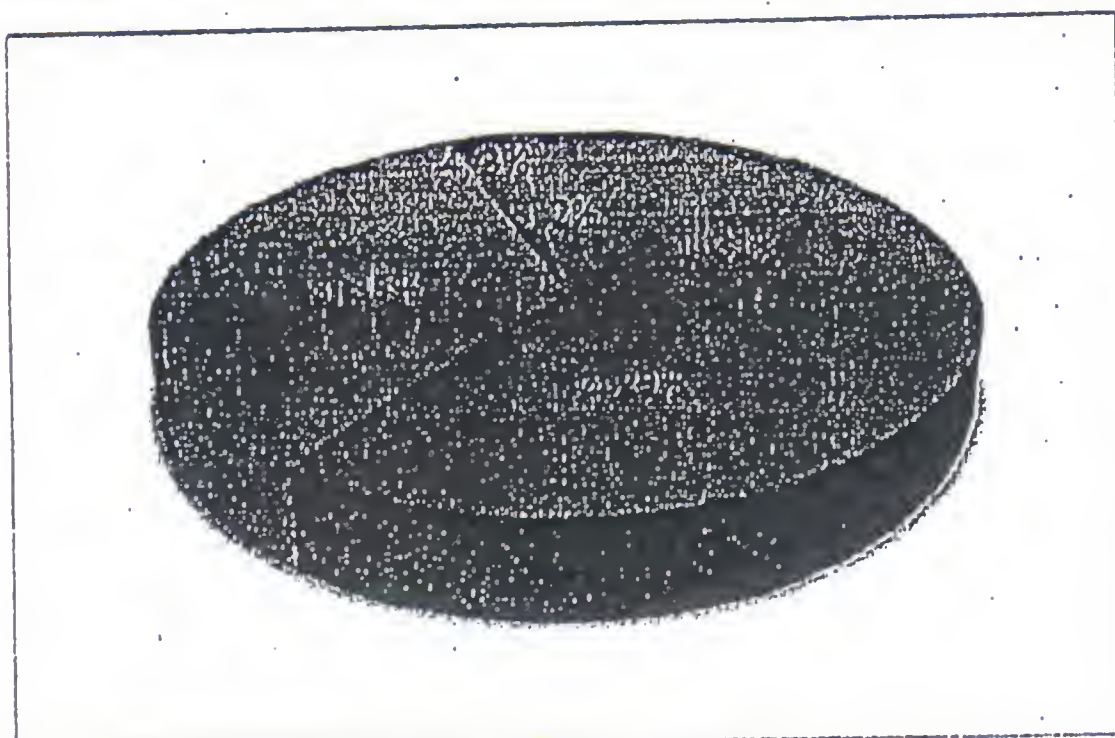


Figure 15 US-VISIT image quality distribution for left index finger

Indian Ground Conditions

The research team at IIIT Delhi focused on the ability to leverage image quality assessment tools in (1) analyzing the input biometric samples that are obtained from diverse; disparate sensors and (2) characterizing the samples based on the quality and amount of information present. Using three fingerprint databases, fingerprint image quality based experimental evaluation was performed.

1. DB1. This database contains images from 27 urban individuals (or 1350 images) and 81 rural individuals (or 1620 images). This database is prepared using single impression sensor meeting FIPS 201 APL and FBI Image Quality Specifications.
2. DB2. Images captured using slap scanner. This database contains slap images from over 20,000 individuals. Each slap fingerprint image was segmented using a commercial segmentation tool. After segmentation, the database contained 200K images. The four-finger slap sensor was EFTS/F certified and operated at level 31.
3. DB3. Pre-segmented rural slap database pertaining to about 5600 individuals (around 56,000 images). The four-finger slap sensor was EFTS/F certified and operated at level 31.

Using DB1, experimental test bed and statistical tests were prepared, followed by evaluation using DB2 and DB3. Using NIST provided Fingerprint Image Quality software (NFIQ), images were classified in to bins according to the image quality score. The bin

167
232

distributions for Indian databases are shown in Figure 16 through Figure 19. Of particular interest is significantly large bin 4 & 5 numbers for DB2 as well as DB1 rural sample. In contract, DB3, another rural area shows exceptionally high bins 1 and 2.

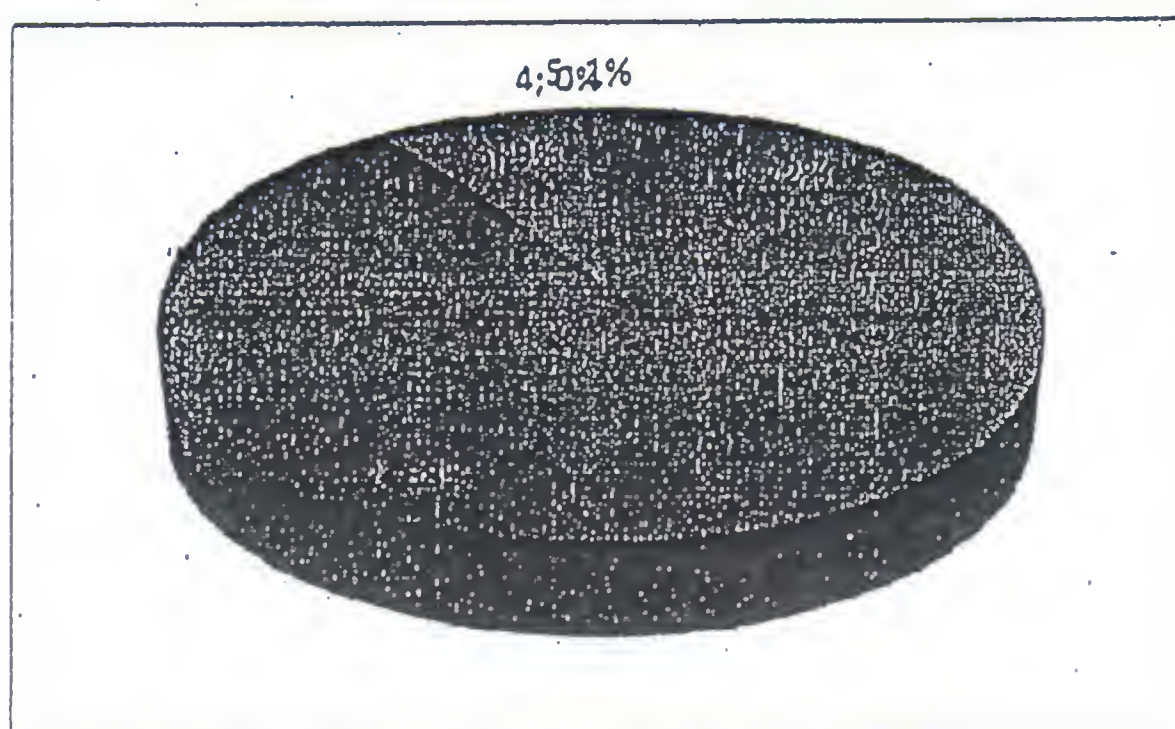


Figure 16 Image quality score distribution for DB1 Urban sample

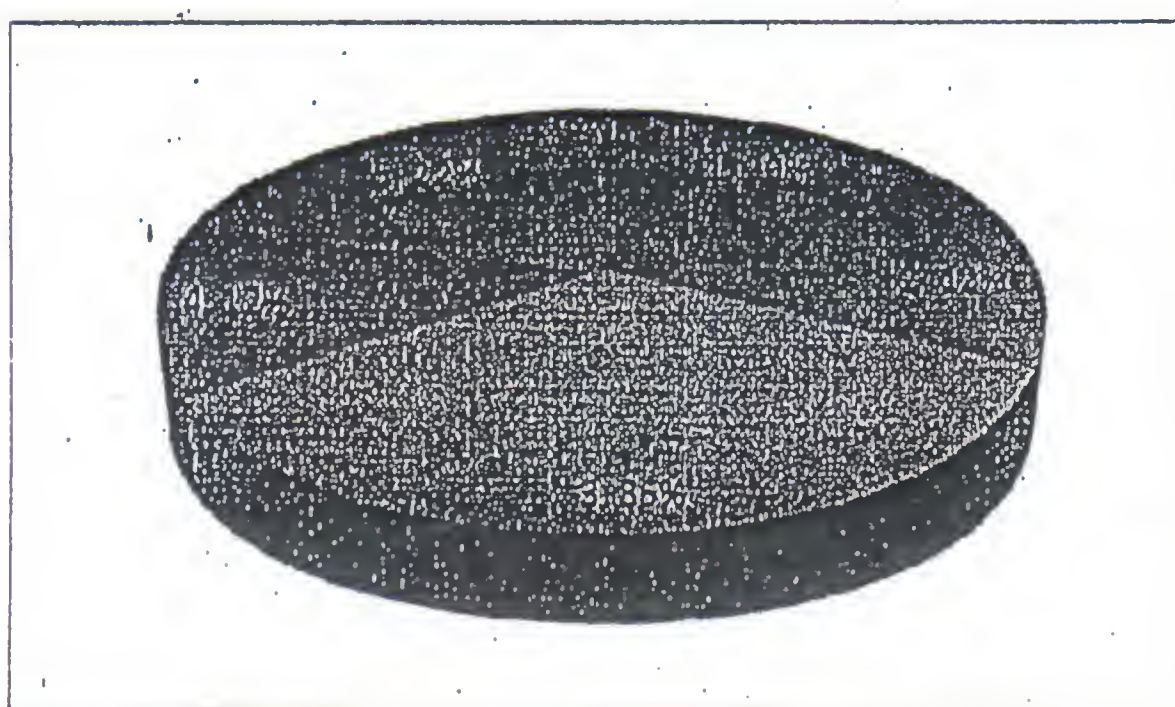


Figure 17 Image quality score distribution for DB1 Rural sample

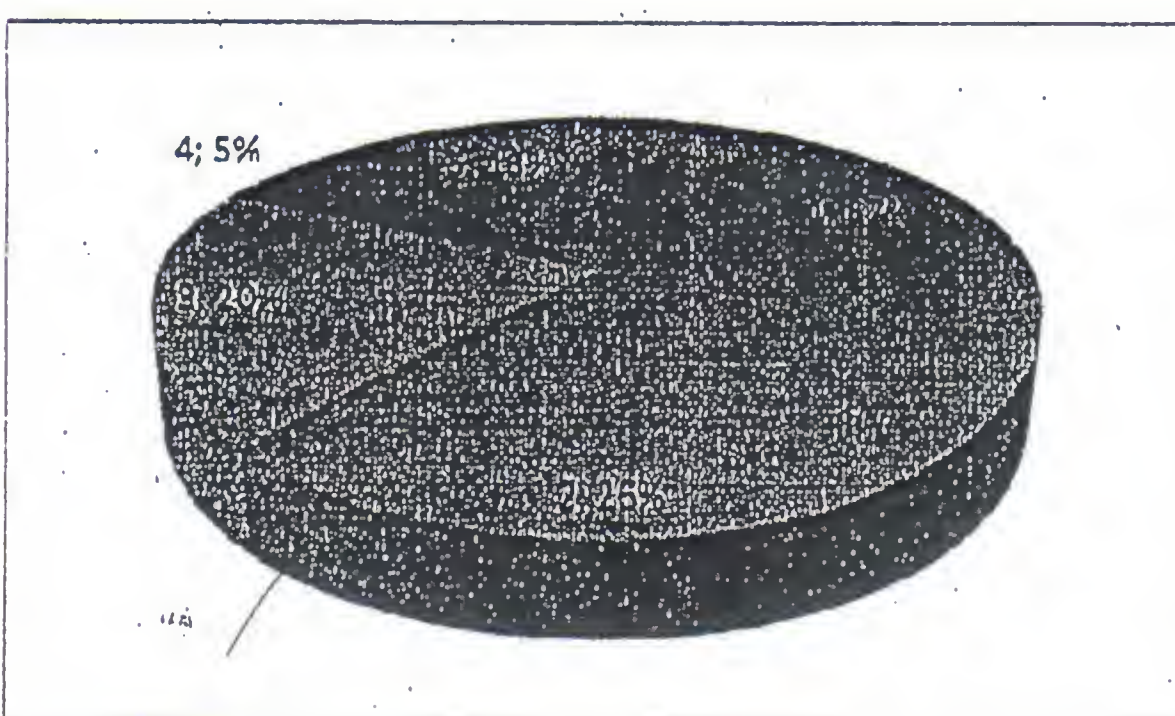


Figure 18 Image quality distribution for DB2

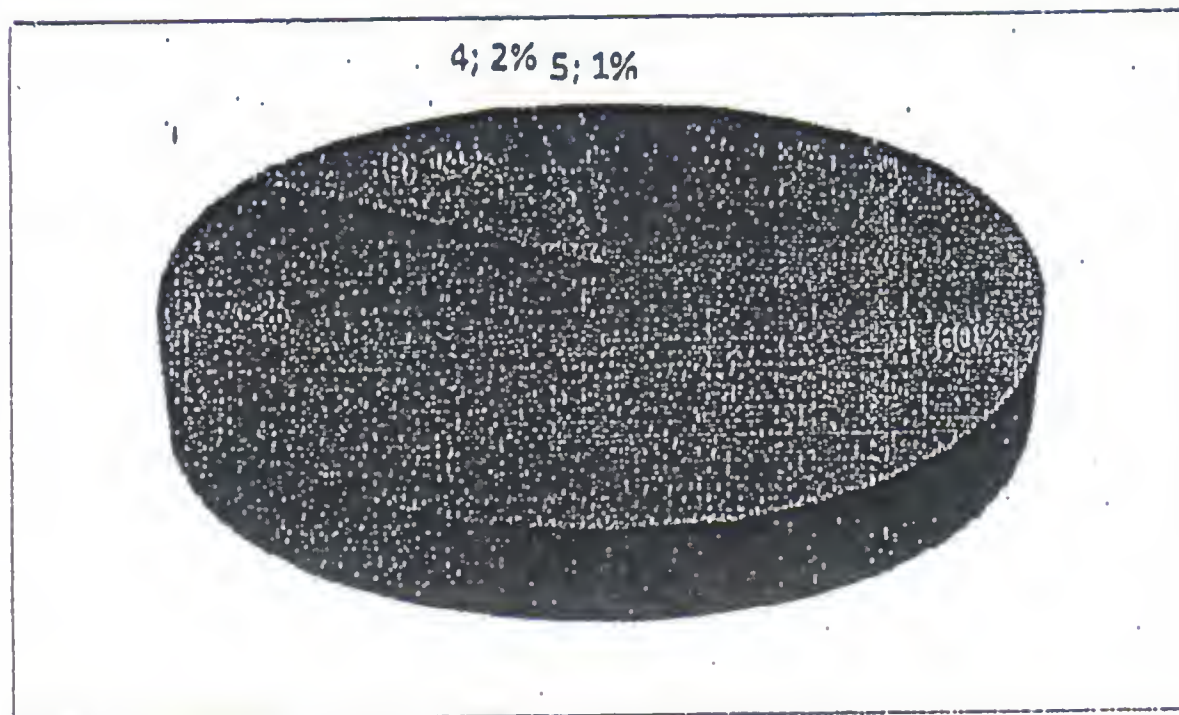


Figure 19 Image quality distribution for DB3

Step 3 Comparison & quality estimates

Since, DB2 and DB3 databases have only a single impression per finger, it is impossible to compute ROC or CMC plots and compute recognition accuracies. However, using existing Western results[24], it is possible to closely predict the expected fingerprint recognition performance.

Figure 20 and Figure 22 compare quality of left and right index finger respectively. Against x axis of accuracy (FAR), it shows cumulative bin score. Line over the Western curve (blue line) indicates that expected accuracy of the sample will be better than that of the Western population. Any points below the Western curve indicate that expected accuracy of that sample will be worse than the Western population.

DB3 shows quality superior to Western image quality while DB2 shows significantly inferior quality. While both samples are from two different rural areas of two different states, the expected accuracy is vastly different.

169
244

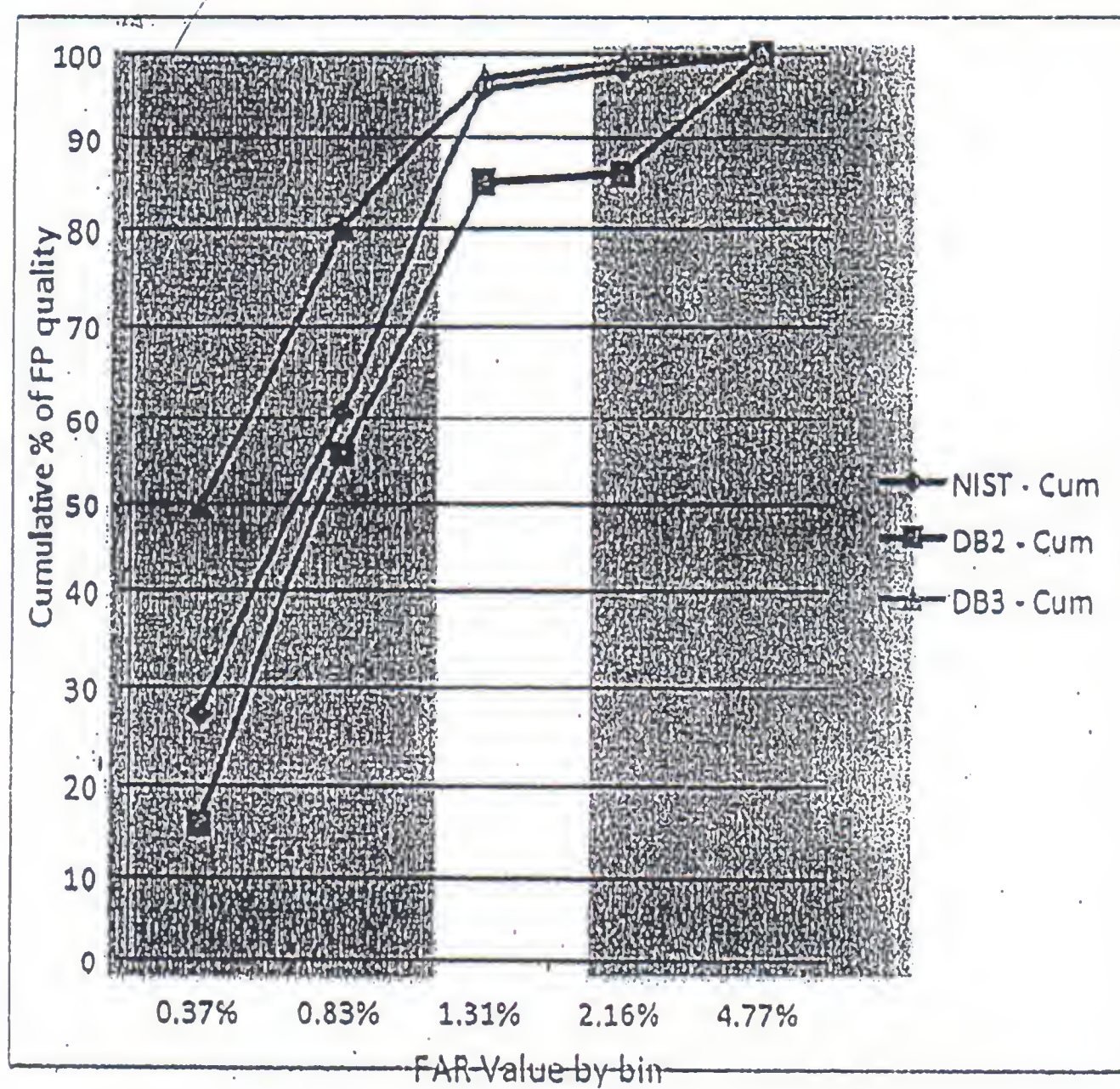


Figure 20 Right-index finger comparison

| Source | Bin 1 | Bin 2 | Bin 3 | Bin 4 | Bin 5 |
|------------|-------|-------|-------|-------|--------|
| | 0.37% | 0.83% | 1.31% | 2.16% | 4.77% |
| NIST | 27.28 | 33.32 | 35.37 | 2.23 | 1.8 |
| NIST - Cum | 27.28 | 60.6 | 95.97 | 98.2 | 100 |
| DB2 | 15.87 | 40.08 | 28.88 | 0.99 | 14.18 |
| DB2 - Cum | 15.87 | 55.95 | 84.83 | 85.82 | 100.00 |
| DB3 | 49.73 | 30.51 | 16.97 | 2 | 0.79 |
| DB3 - Cum | 49.73 | 80.24 | 97.21 | 99.21 | 100.00 |

Figure 21 Right index finger numerical data

170
245

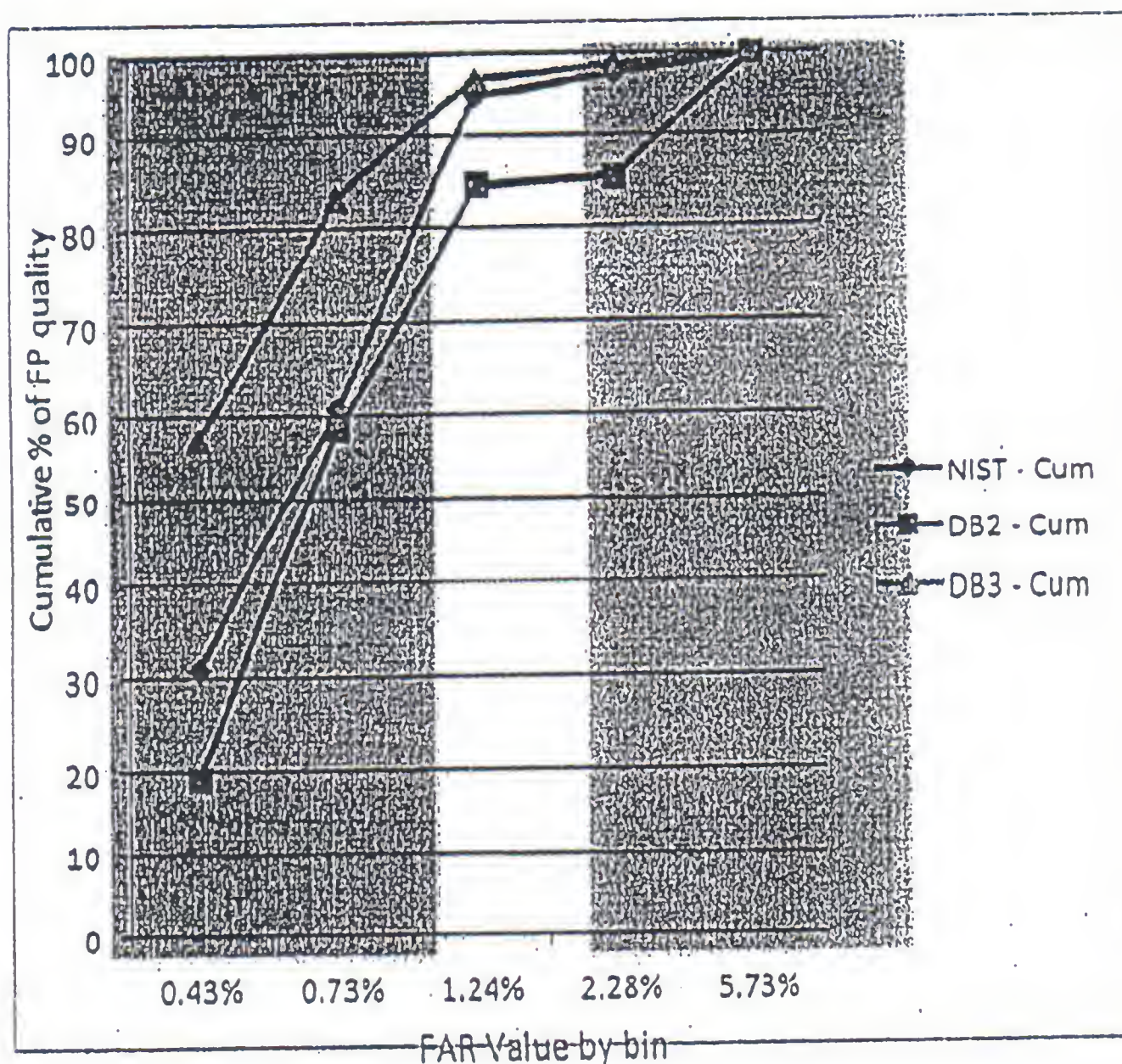


Figure 22 Left index finger comparison

| Source | Bin 1 0.43% | Bin 2 0.73% | Bin 3 1.24% | Bin 4 2.28% | Bin 5 5.73% |
|------------|----------------|----------------|----------------|----------------|----------------|
| NIST | 30.83 | 29.78 | 34.08 | 2.88 | 2.43 |
| NIST - Cum | 30.83 | 60.61 | 94.69 | 97.57 | 100 |
| DB2 | 18.99 | 39.36 | 25.87 | 0.90 | 14.88 |
| DB2 - Cum | 18.99 | 58.35 | 84.22 | 85.12 | 100.00 |
| DB3 | 57.25 | 25.77 | 13.8 | 1.87 | 1.31 |
| DB3 - Cum | 57.25 | 83.02 | 96.82 | 98.69 | 100.00 |

Figure 23 Left index finger comparison

Conclusions

NFIQ results on the databases seem to be encouraging especially if the fingerprint images are captured using good operational processes. For the majority of images, quality scores vary from excellent to good. Using these images, the typical performance of fingerprint feature extraction and matching should meet expectations. Therefore, to achieve good recognition accuracy, good quality images should be collected using optimized operational mechanisms and good sensors.

- The UIDAI can achieve fingerprint accuracy of a quality similar to developed countries. There is good evidence to suggest that Indian rural data may be as good as developed country settings when proper operational procedures are followed and good quality devices are used.
- It is possible to closely predict the expected fingerprint recognition performance. In the experiments, it is observed that, at 95% confidence, DB2 is expected to show lower accuracy compared to the Western data whereas DB3 is expected to achieve similar accuracy (for $Q = 1, 2$, and 3 , 99% TAR with about 1% FAR).

171
246

- It is believed that DB3's improved image quality is due to better operational procedures. A few simple methods were used in DB3 data collection, such as:

1. Using wet towels to remove dirt and moisten dry fingers
2. Using minimum quality threshold to ensure that extra efforts are made to capture good prints from hard to obtain fingers and
3. Keeping scanning devices in operational order

These resulted in exceptionally good bin 1 and 2 distribution.

- It is also observed that the slap fingerprint segmentation tools require some prior training for Indian databases. After some training, segmentation results improve by 2-3%. This also suggests that in deploying a biometrics (fingerprint) system, a carefully designed a priori training set and procedure will help in improving performance.
- Since NFIQ tool is trained using Western data, there are around 4-5% errors in correctly assigning the quality scores in the Indian fingerprints. It might be possible to tune the tool to Indian data.
- When the fingerprint images in DB1 (rural and urban setting), specifically those causing errors were analyzed, it was found that there are some specific causes that are more relevant in the Indian sub-continental region compared to Western and European countries. Lawsonia Inermis (commonly known as henna or mehendi) can cause significant differences in the quality of fingerprint images. Widely used by women in the Indian sub-continent during festivals, henna is applied on hand/fingers and when applied, fingerprint sensors may not properly capture fingerprint features.
- On analyzing the quality distribution of each finger in every age group, it is difficult to generalize little fingers as useful or not. Similarly, it is not possible to generalize that, a particular age group or gender conforms to lower or higher quality scores and hence better/worse performance.

Finally, it is strongly recommended that carefully designed experiments and proper statistical analysis under pilot should be carried out, to formally predict the accuracy of biometric systems for Indian rural and urban environments.

Face Identification

Face image, uncorrelated to fingerprint image, can be utilized in two ways. Face image can be independently matched using automatic matching algorithm and the results fused together to achieve higher net accuracy. NIST reports improved accuracy using fingerprint and face image score fusion [28]. It should be noted that face image alone provides low accuracy rate. A more practical method is hierarchical matching where false match rate can be improved by comparing face images of suspected duplicates obtained in fingerprint matching. In the former, the entire database has to be used as gallery, making the matching prohibitively expensive. In the later, gallery size is small, typically 1% of database. The hierarchical method improves FRR (which reduces manual duplicate check) but does not directly improve FAR (which results in duplicates in the database). However, one can trade off FRR to improve FAR.

172
247

Iris

Iris has been shown to provide accuracy comparable to fingerprint. NIST Iris test provided accuracy rates shown in Figure 24[10]. T. Mansfield of National Physical Laboratory [33] reports low FAR for small sample.

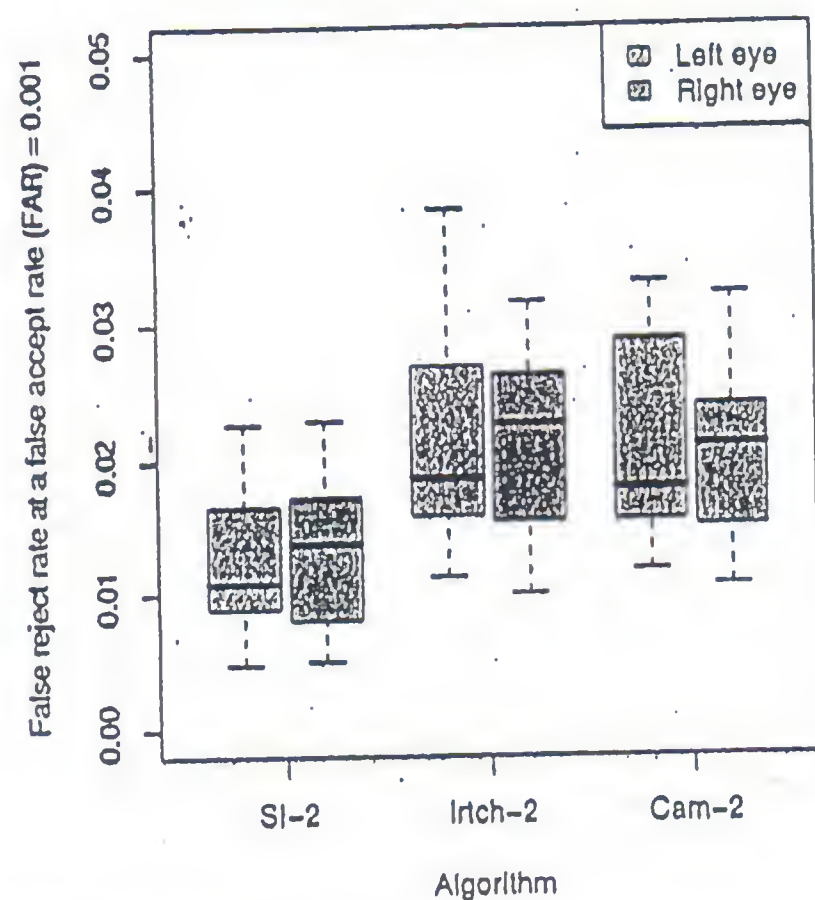


Figure 24 Iris FAR & FRR rate

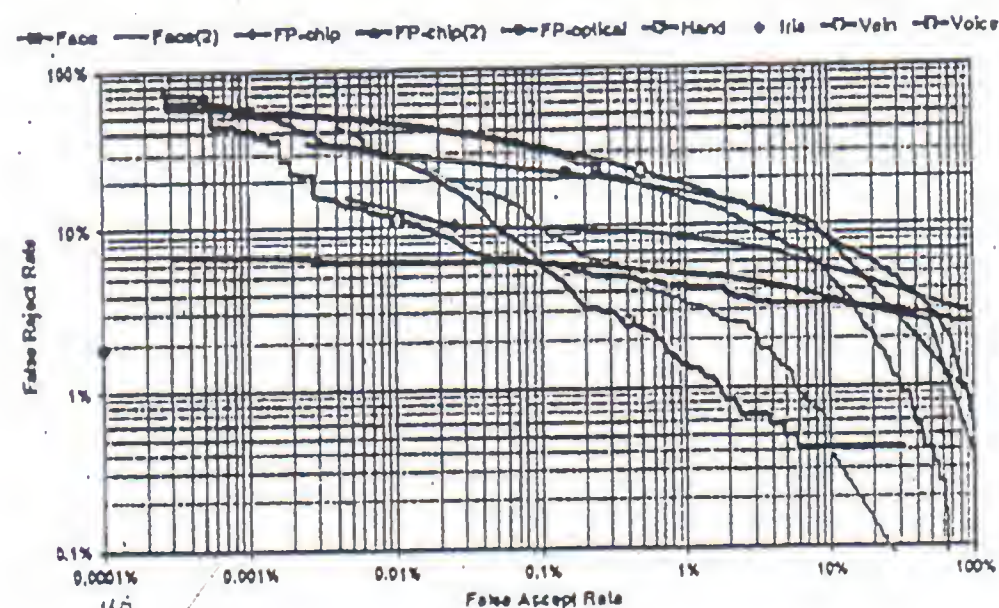


Figure 25 FAR and FRR of various biometric identifier

Fused Accuracy

A large body of literature documents the benefits of information fusion in a variety of fields including search, data mining, pattern recognition, and computer vision. Fusion in biometric is an instance of information fusion. A strong theoretical base as well as numerous empirical studies has been documented that support the advantages of fusion in biometric systems [1]. The main advantage of fusion in the context of biometrics is an improvement in the overall matching accuracy. Depending on the fusion method, the matching speed may also be improved significantly. Dr. Phalguni Gupta and his team report a study of fusion of fingerprint with iris [7]. They show a substantial improvement in matching accuracy by combining one iris with one finger. There is no empirical data available for Indian conditions though there is strong theoretical evidence that among all economically and technically feasible biometrics modalities,

173
248

combined fingerprint and iris has potential to provide maximum accuracy in Indian conditions.

174
249

ISO Documents

Included by reference

ISO/IEC 19794-2:2005. Biometric data interchange formats – Part 2: Finger minutiae data

ISO/IEC 19794-4:2005. Biometric data interchange formats – Part 4: Finger Image data

ISO/IEC 19794-5:2005. Biometric data interchange formats – Part 5: Face Image data

ISO/IEC 19794-6:2005. Biometric data interchange formats – Part 6: Iris Image data

175
250

References

1. A. A. Ross, K. Nandakumar, A. K. Jain, Handbook of Multibiometrics, Springer, 2006
2. Anil Jain, Patrick Flynn, Arun Ross. Handbook of Biometrics, 2008
3. ANSI/NIST-ITL 1-2007. American National Standard for Information Systems—Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 1
4. ANSI/NIST-ITL 2-2008. American National Standard for Information Systems—Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 2 XML Version
5. Bolle, Connell et al. Guide to Biometrics, 2004
6. Fingerprint Image Data Standards for Indian e-Governance Applications, Draft Version 0.4, National Information Center
7. H. Mahrotra, A. Rattani, P. Gupta, "Fusion of Iris and Fingerprint Biometric for Recognition", Proceedings of International Conference on Signal and Image Processing (ICSIP 2006), Karnataka, India, 2006
8. IAFIS-IC-0100 (V7) Electronic Fingerprint Transmission Standard (EFTS) 1999
9. International Biometrics Group, "Independent Testing of Iris Recognition Technology, Final Report, May 2005", NBCHC030114/0002. Study commissioned by the US Department of Homeland Security.
10. IREX I, "Performance of Iris Recognition Algorithms on Standard Images", NIST Interagency Report 7629
11. ISO/IEC 19784-1:2006. Biometric Application Programming interface – Part1: BioAPI specification.
12. ISO/IEC 19794-1:2006. Biometric data interchange formats – Part 1: Framework
13. ISO/IEC 19794-5:2005. Biometric data interchange formats – Part 5: Face image data
14. ISO/IEC 19794-6:2005. Biometric data interchange formats – Part 6: Iris image data
15. J. Cambier, "Iridian Large Database Performance", Iridian Technical Report 03-002
16. J. Daugman, "Algorithms, Performance & Challenges", BYSM, 2006
17. J. Daugman, "Iris recognition border crossing system in the UAE", International Airport Review (2) 2004.
18. J. Daugman, Technical Report 635, University of Cambridge, 2005
19. James Matey, "Iris Recognition", Sarnoff Corporation, BCC 2005
20. Jonathon Phillips, "ICE 2006 Large-Scale Results", NIST 7208, NIST, 2007
21. NISTIR 7110. Matching Performance for the US-VISIT IDENT System Using Flat Fingerprints. C. L. Wilson, M. D. Garris, & C. I. Watson, May 2004
22. NISTIR 7112. Studies of Plain-to-Rolled Fingerprint Matching Using the NIST Algorithmic Test Bed (ATB); Stephen S. Wood & Charles L. Wilson, April 2004
23. NISTIR 7123. Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report, Charles Wilson et al.
24. NISTIR 7151. August 2004 Fingerprint Image Quality
25. NISTIR 7201. Effect of Image Size and Compression on One-to-One Fingerprint Matching. C. I. Watson & C. L. Wilson. February 2005

- 176
251
26. NISTIR 7249. Two Finger Matching With Vendor SDK Matchers. C. Watson, C. Wilson, M. Indovina & B. Cochran. July 2005
 27. NISTIR 7296. MINEX. Performance and Interoperability of the INCI TS 3 7 8 Fingerprint Template. Patrick Grother, Michael McCabe et al. March 2006
 28. NISTIR 7346 TR. Studies of Biometric Fusion, 2007
 29. Patrick Grother, Elham Tabassi, "Performance of Biometric Quality Measures", IEEE transactions on pattern analysis and machine intelligence, Vol. 29, No. 4, April 2007.
 30. Registry of USG Recommended Biometric Standards, Version 2.0, NSTC
 31. Report of the working group on standards for raw images of fingerprints, Reserve Bank of India
 32. Shahram Orandi, Mobile ID Device Best Practice Recommendations, NIST Special Publication 500-280, August 2009
 33. T. Mansfield, G. Kelly, D. Chandler, J. Kane, "Biometric Product Testing Final Report", CESG Contract X92A/4009309, Centre for Mathematics & Scientific Computing, National Physical Laboratory, Queen's Road, Teddington, Middlesex TW11 0LW
 34. UK Passport Service, Biometrics Enrolment Trial, May 2005



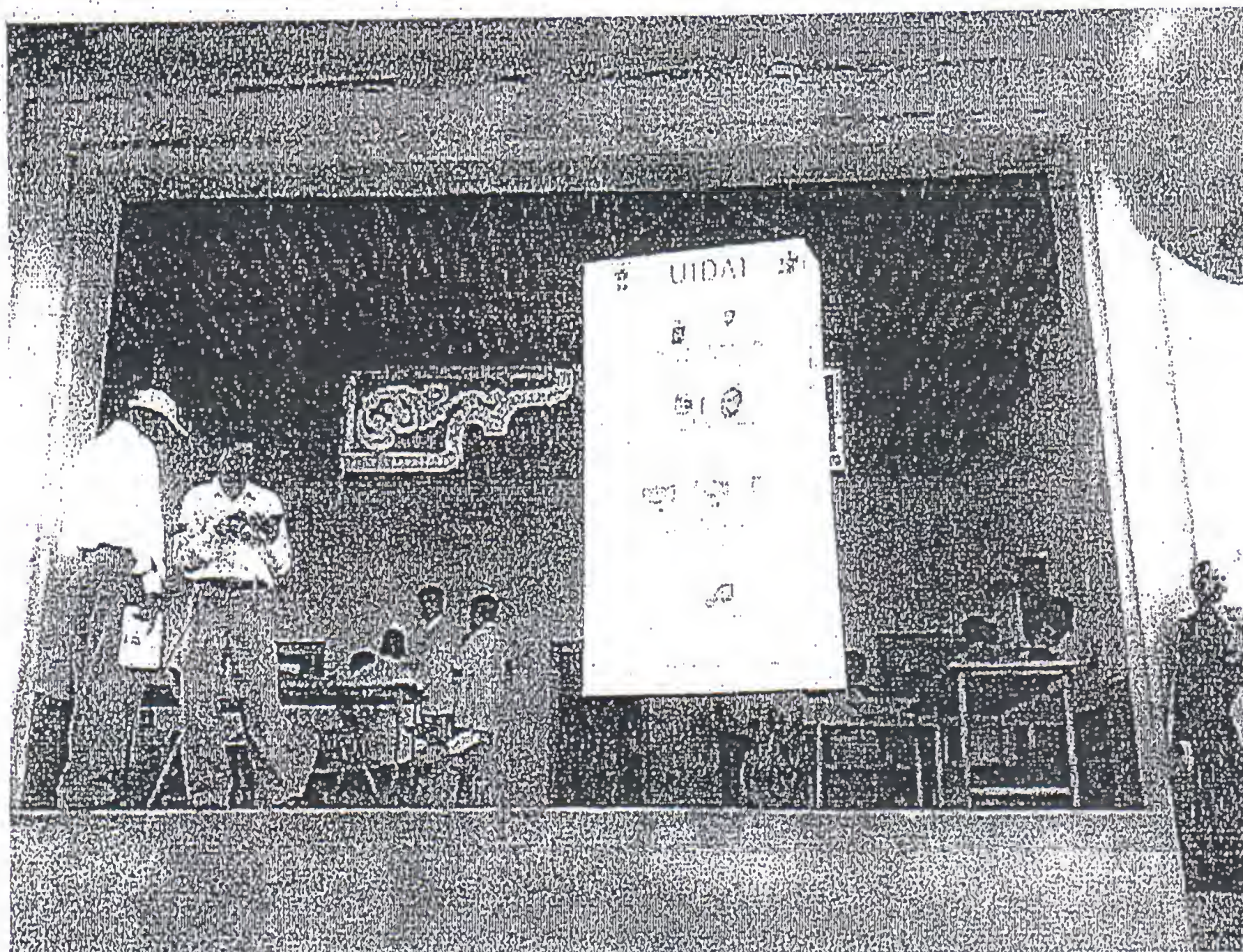
UIDAI

Unique Identification Authority of India
Planning Commission, Govt. of India (Gol),
3rd Floor, Tower II,
Jeevan Bharati Building,
Connaught Circus,
New Delhi 110001

177

252

ANNEXURE R-16



UID Enrolment Proof-of-Concept Report

178
253

Table of Contents

| | |
|--|------------------------------|
| Introduction | 3 |
| Goals | Error! Bookmark not defined. |
| Executive summary of outcome | 4 |
| Chronology of planning and execution | 5 |
| Choice of locations | 5 |
| Biometric devices | 9 |
| Preparation of enrolment agency and software | 9 |
| Pre-enrolment field and data preparation | 10 |
| Enrolment Process | 13 |
| Process Variations | 14 |
| Enrolment software | 16 |
| Reenrolment Rates | 17 |
| Observations | 19 |
| Process observations | 20 |
| Biometric observations | 22 |
| Conclusion | 24 |
| Annexure 1 - Enrolment application screen shots | 25 |
| Annexure 2 – Enrolment times by age and demographics | 29 |
| Enrolment times by age | 29 |
| Enrolment times by occupation | 29 |
| Enrolment times by gender | 29 |
| Annexure 3 – Biometric matching accuracy curves | 30 |

Introduction

The UID Authority of India conducted a Proof-of-Concept (PoC) study of biometric enrolment from March 2010 to June 2010 in the predominantly rural areas of Andhra Pradesh, Karnataka, and Bihar. The UIDAI also carried out the biometric enrolment of school children in the vicinity of Bangalore. About seventy five thousand people in all were enrolled during the first phase of the PoC study, and sixty thousand of the same people were re-enrolled during the second phase after a gap of three weeks.

Prior to conducting the UIDAI PoC, there was insufficient reliable biometric data available for residents of India that could be used to analyze and reach conclusions relevant to the implementation of the UID program. In addition, outside the state of Andhra Pradesh, there was no significant history of collecting iris images. In the last five years, iris image capture devices have gone through significant technological advances. There was however, limited data available from anywhere in the world regarding the ease of iris capture, as well as the usability of iris images in the case of minors. Therefore, the UIDAI felt it necessary to conduct Proof-of-Concept studies for biometric enrolment in several states, and analyze the data.

This report chronicles these Postludes. The report consists of a narrative of the activities, observations and conclusions based on numerous visits to the enrolment sites, and conclusions inferred through i) the statistical analysis of the processes and ii) by biometric analysis of the data collected during the studies.

In the study, face photos, iris images, and fingerprints of all ten fingers were captured. The ten fingerprints were captured in two different ways: first using a slap device, and then using a single finger device. Rural areas were emphasized in the study for two reasons. One was the uneven quality of fingerprints expected from rural workers whose fingerprints could be worn out by prolonged physical labour. The second was to test the UIDAI's ability to carry out biometric enrolment in locations representative of the majority of India's infrastructure, i.e. in areas with limited access to electrical power, proper lighting, and other support systems.

Objectives

The enrolment PoC was conducted to evaluate technical, operational, and behavioural hypotheses related to both the use of biometric devices and the overall enrolment process itself. It was also conducted to establish a baseline for the quality of biometric data that could be collected in rural India.

Technical objectives

- i) Measure the biometric quality that could be achieved in rural Indian conditions
- ii) Understand the difficulty challenges in capturing iris images,

180
255

iii) Determine suitable ergonomics in the use of the biometric devices, and understand the optimal overall layout of the enrolment station.

Operational objectives

i) Carry out a time and motion study through observation, as well as analysis of process data collected through the client software.

Behavioural objectives

i) Understand how people in rural India would respond to the capture of iris images. This was an important goal, since data on the experience of the public with iris capture devices is limited, compared to studies on fingerprint capture.

ii) Overall response of enrolees to the entire biometric capture process in the PoC needed to be understood

There were also more intangible lessons that would be directly applicable to the actual UID enrolment; since the PoC was designed to mimic UID enrolment. For instance, it was expected that the PoC experience would enable the UID team to tailor biometric enrolment best practices to be more applicable in Indian conditions.

Executive summary of outcome

1. The PoC successfully conducted over 135,000 biometric enrolments. The relative ease of conducting the operation confirmed that biometric enrolment conforming to UID standards of quality and process was indeed possible on a large scale in rural India. The total biometric enrolment time for each individual, on average, was a little over three minutes. Of this, iris enrolment took a little under a minute, and was not perceived to be excessively difficult either by the resident or the enrolling operator. Specifically, many blind people had their iris images captured (For details, see table Page 19)
2. Multiple fingerprint scanners as well as iris capture devices were used in the PoC, and they performed according to expectations. The PoC was dispersed geographically and included many rural, often remote locations across three states. The enrolment was typically conducted with minimal infrastructure and sometimes in extreme weather conditions. Enrolees varied in age all the way from four years to about ninety years of age.
3. Older people took longer to enrol than younger people, and enrolees whose employment involved manual work took longer to enrol than the rest of the PoC population. Older people needed more assistance from operators to capture of their

181
256

biometrics. However, the range of enrolment times observed was well within expectations and was not seen as making enrolment impractical.

4. The enrolment variations tested in the process led to the conclusion that the best process was one where the enrollee remained stationary during enrolment and the operator did the positioning of the devices.
5. The enrolment of children in the school showed that children in the age range of four to fifteen could be biometrically enrolled using the same process as that used for adults and with no additional difficulty. The match analysis also showed that their iris images and fingerprints could be deduplicated as accurately as those of adults.
6. The quality of the biometric capture was sensitive to the setup of the enrolment station and the process itself. Most importantly, the enrolment operator's instructions made a significant difference in the efficiency of the biometric capture.
7. The quality check process built into the enrolment software was very important and provided helpful feedback to the operator in capturing high quality images.
8. The biometric matching analysis of 40,000 people showed that the accuracy levels achieved using both iris and ten fingerprints were more than an order of magnitude better compared to using either of the two individually. The multi-modal enrolment was adequate to carry out deduplication on a much larger scale, with reasonable expectations of extending it to all residents of India.

Chronology of planning and execution

It was decided that the PoC would be done in three states: Andhra Pradesh, Karnataka, and Bihar. At least 20,000 sets of biometric data had to be collected in each state. To analyze the accuracy of biometric matching, the same set of biometric samples had to be collected again after a suitable time lag of three weeks. In order to ensure that the 20,000 sets of duplicate data could be collected, the initial enrolment target in each state was 25,000. This would allow for a minority of people not showing up for re-enrolment during the second round.

The regional offices of the UIDAI in conjunction with the technology team worked with the state governments to plan the PoC. In Andhra Pradesh and Karnataka, the Food & Civil Supplies department was designated the nodal agency for the PoC study. In Bihar, the PoC was done in conjunction with enrolment for the NREGS e-Shakti project.

Choice of locations

The following factors were considered while choosing locations for the PoC:

- i) The enrollees at the PoC locations had to be representative of the Indian population in biometric quality. This meant that over eighty percent of the PoC locations

182
57

- were rural, since the majority of India lives in villages. However, the remaining twenty percent of the PoC sites were urban locations close to large cities, in order to have urban areas well represented in the biometric samples collected.
- ii) A further consideration was that the rural locations should be at least fifty kilometres away from the large metropolitan areas, such as Bangalore or Hyderabad. This was done since a sampling of closer locations showed that the working population of the villages close to metropolitan areas typically commuted to urban locations for work, and in general, the population was more representative of urban populations.
 - iii) The goal of the PoC was to collect data representative of India and not necessarily to find difficult-to-use biometrics. Therefore, extremely remote rural areas, often with populations specializing in certain types of work (tea plantation workers, areca nut growers, etc.) were not chosen. This ensured that degradation of biometrics characteristic of such narrow groups was not overrepresented in the sample data collected.
 - iv) For the three PoCs (apart from the school PoC), the goal was to enrol adults. In Karnataka and Bihar, only residents above 18 years were allowed to enrol. In Andhra Pradesh, adults were encouraged to enrol and very few minors actually enrolled.

The state nodal agencies in collaboration with the UID team and the enrolment agencies accordingly selected a set of locations to conduct the PoC. In Andhra Pradesh and Karnataka, two districts each were chosen for the PoC. In each district, five villages were selected for enrolling people. In Bihar, the villages scheduled for PoC enrolment was decided by the e-Shakti schedule.

The PoC was subsequently conducted in ten villages each in Karnataka and Andhra Pradesh, and in over thirty villages in Bihar. The choice of villages across states met our goal of geographic diversity since the PoC locations were widely dispersed

Within each village, the enrolment location selected was usually the local primary school or other public building (photos below). The enrolment agency brought computers, biometric devices and related equipment. In most areas, one or two power generators were also brought to provide reliable power for lighting and computers. The enrolment was carried out using locally available furniture.

PoC enrolment was also conducted in the Deputy Commissioners' offices in Mysore and Tumkur cities. Finally, PoC enrolment for school children between 4 years and 15 years was conducted in a Bangalore school. In Karnataka, the villages chosen were those with Gram Panchayat offices, i.e., larger villages. In Andhra Pradesh and in Bihar, this was not always so. The following is the list of PoC locations.

183
258

| Bihar | | |
|----------------|--|----------|
| Gram Panchayat | Revenue Villages | Block |
| Bind | Bind (ward no. 4-14) Bind (Kusa, Bishunpur and Nirachak) | Bind |
| Jahana | Jahana, Chatapur, Rampur, Nipur, Khalsa, & Nigraan | Bind |
| Jamra | Barhag, Jamra, & Darapur | Bind |
| Kamra | Kamra, Jekki, Bakra, Makapur, & Makapur (Dhulapur) | Bind |
| Lodpur | Lodpur, Jaitpur, Gajpur, Ibrahimpur | Bind |
| Onda | Onda | Asthawan |
| Tajpur | Tajpur, Mahmudabad, Madanchak, Rasapur, Nauranga, & Rajpur | Bind |
| Utarchu | Utarchu, Masia, Ahachak, Mufipur | Bind |

| Andhra Pradesh | | |
|----------------|------------------|-------------------------|
| District | Mandal | Village |
| Medak | Tupran | Ghanpur |
| | Wargal | Wargal |
| | Wargal | Veluru |
| | Chegunta | Narsingi |
| | Patancheru | Ward-11 |
| Krishna | Mylavaram | Velvadam |
| | Kruthivennu | Lakshmi puram |
| | Vijayawada Rural | Nidamanuru |
| | Penamaluru | Poranki |
| | (Urban) | Vijayawada Urban Ward 9 |

| Karnataka | | |
|-----------|-----------|------------------------------|
| District | Taluk | Gram Panchayath or DC Office |
| Tumkur | Tumkur | DC Office Staff |
| | Tumkur | Bellary |
| | Gubbi | Chelur |
| | Madhugiri | Doddur |
| | Tiptur | Kibbanahalli |
| | Sira | Bukkapatna |
| Mysore | Mysore | DC Office Staff |
| | Mysore | Varpna |

184
259

| | | |
|-----------|-----------------------|---------------------|
| | HID Kote | Hommaragalli |
| | Nanjangud | Hadinaaru |
| | Hunsur | Gowdagere |
| | KR Nagar | Lippuru |
| Bangalore | School (children PoC) | Pooma Prajna school |



Figure 1 Typical PoC Enrolment location

125
260

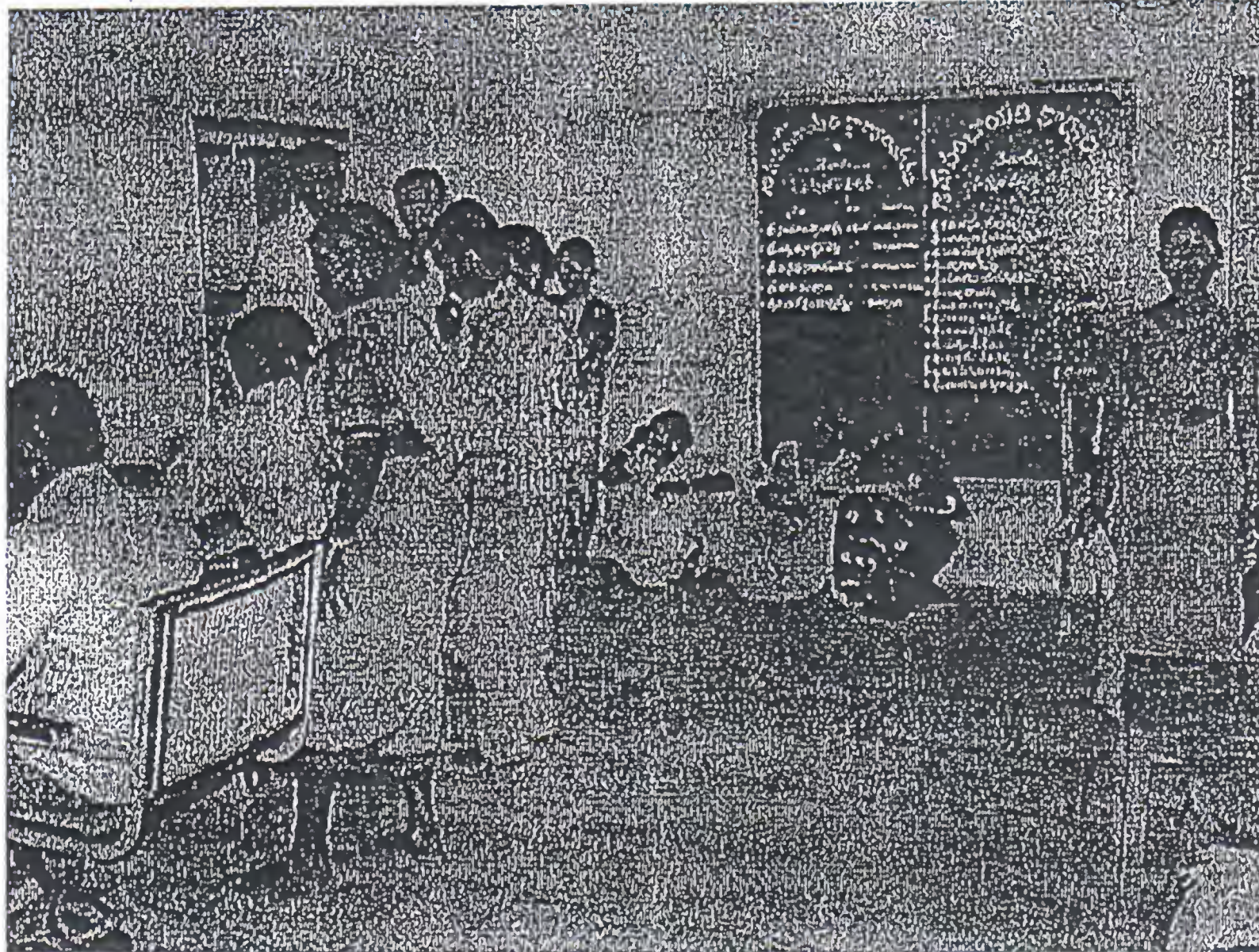


Figure 2 Typical PoC Enrolment room

Biometric devices

Fingerprint scanners and iris capture devices from three different vendors were used in the three PoC states. In Karnataka, the iris devices were from Iris ID (formerly LG Iris) and the fingerprint devices were from Morpho (formerly Sagem). In Bihar, the fingerprint scanner and the iris capture device were both from Crossmatch Technologies. In Andhra Pradesh, the fingerprint scanner and iris capture devices were both from L-1 Identity solutions. In Andhra Pradesh, both a single-eye iris capture device and a two-eye iris capture device were used. The Crossmatch iris devices were binocular type, the L-1 Iris devices were hand-held, and the Iris ID iris devices were mounted on tripods, but could also be used as hand-held devices. Using multiple devices added further to the diversity of the PoC process and later enabled us to match images captured using different devices.

Preparation of enrolment agency and software

Enrolment agencies who had already worked with the respective states on previous projects were chosen to implement the PoC by the respective state government agencies. The agencies were 4G ID solutions in Andhra Pradesh, Comat Technologies in Karnataka, and SmarTech Technologies (an arm of Glodyne) in Bihar. In parallel, biometric devices were procured for the PoC. The biometric devices procured were the following: iris capture devices, iris and face capture devices, slap fingerprint scanners, and single finger capture devices.

The enrolment agencies had varying levels of biometric enrolment experience. The UID technology group worked with each agency to ensure adequate training and prescribed the process flow to be followed.

186
261

A reference implementation of the enrolment software was created to standardize the process and have a uniform look-and-feel of the application across all three states. However, since the devices used were different in each state, the enrolment software used in each state was a custom version which followed the reference design. The UID technology team worked with each of the three agencies to create the customized software to be used in the corresponding state. There were also variations in the capture process followed, particularly in iris capture, because of the variations in capture devices.

A special feature of the enrolment software was that all biometric images went through a software quality check process. The quality check would indicate a pass or fail based on minimal acceptable quality of the image. If the quality check failed, the image would still be stored, but the operator would be required to recapture the image. The enrolment software entailed the operator to repeat the capture up to four times. The software ensured that the operator was not able to proceed to the next step until the recapture was done.

One important aspect of the enrolment software was the capture of process data along with biometric and demographic data. Thus the number of capture attempts and timestamps captured at numerous points in the capture process were written into an XML file during enrolment. This enabled us to eventually carry out a detailed analysis of the process.

Pre-enrolment field and data preparation

The initial step was to work with the local authorities to find possible enrolment locations and make preparations for getting people to show up. The local authorities typically went house-to-house to inform residents about the date and time they were to enrol. The authorities would also be present at the enrolment centre to ensure that people did show up, resolve any disputes among the enrolees and maintain order. The part played by the local authorities was consequently crucial to the success of the enrolment drive.

The enrolment agency supervisors visited the locations to identify the most suitable building for the enrolment centre, ahead of the start of the PoC. They also arranged for the right furniture among what was available in the building and set up the enrolment stations to meet the PoC needs. One important point was that the table should not be too wide and the heights of the operator, and size of the chairs for the enrolee should accommodate the biometric capture process.

Additionally, it was ensured that there was adequate space for people to wait outside since people crowding around the biometric stations would disturb the process. However, a few chairs were kept nearby for observers since it was felt that each resident observing the process before his or her enrolment would improve the person's ease of enrolment. Posters describing the biometric process (shown in photograph below) were also put up at the door of the enrolment centre to help enrolees familiarize themselves with the process.

In parallel, the demographic data of the residents of the local taluk or mandal was obtained from the food and civil supplies department and loaded into the appropriate laptops. Blank

187
262

forms were also kept at the enrolling centres to accommodate people who did not appear in the database, but wished to enrol.

Provisions were made for a bucket of water and towels for residents involved in manual work to clean their hands before enrolment. Also wet and dry clothes were kept at each enrolment station for assisting people with overly dry fingers.

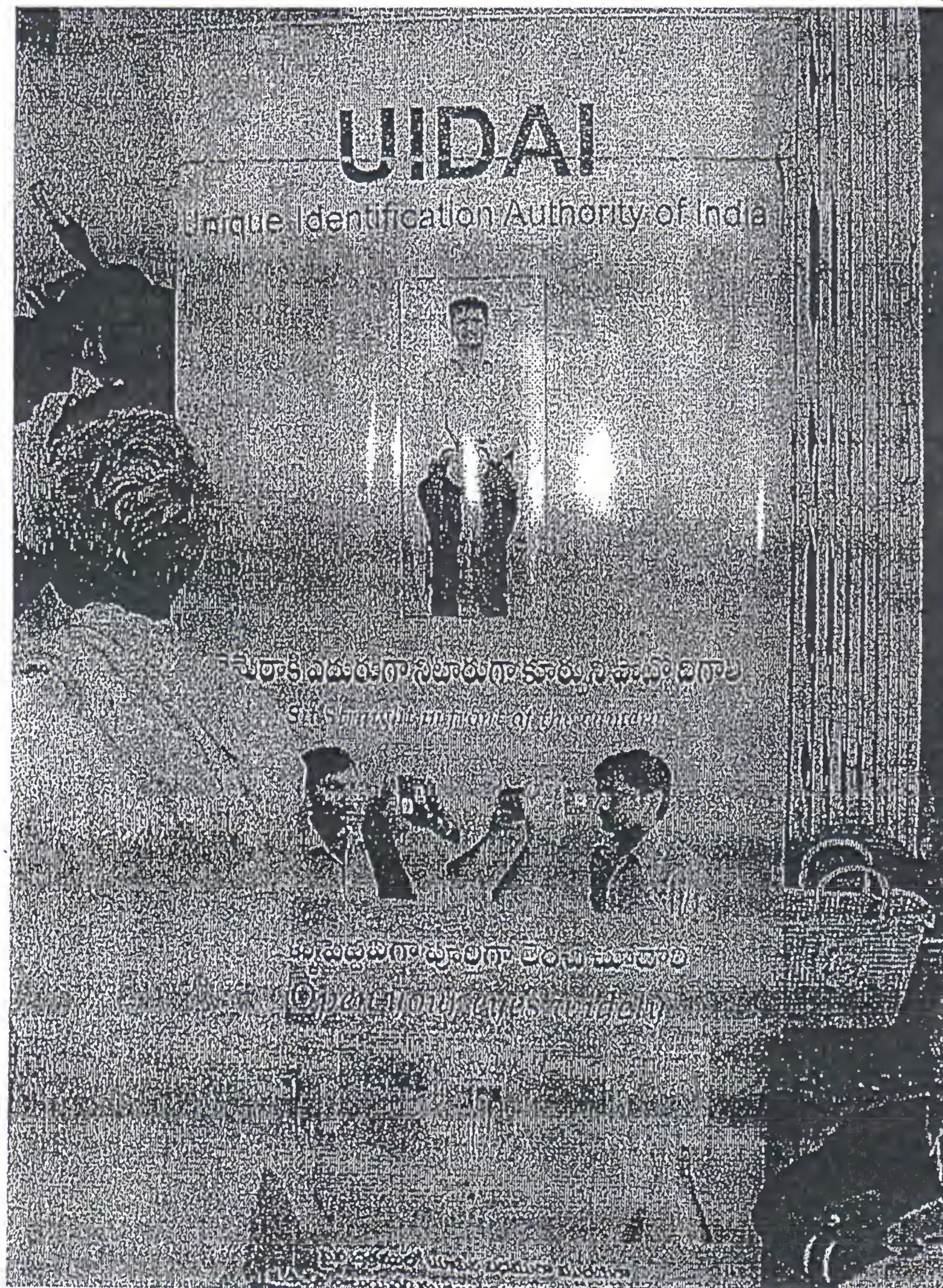


Figure 3 Poster describing biometric capture for residents to observe

189
263

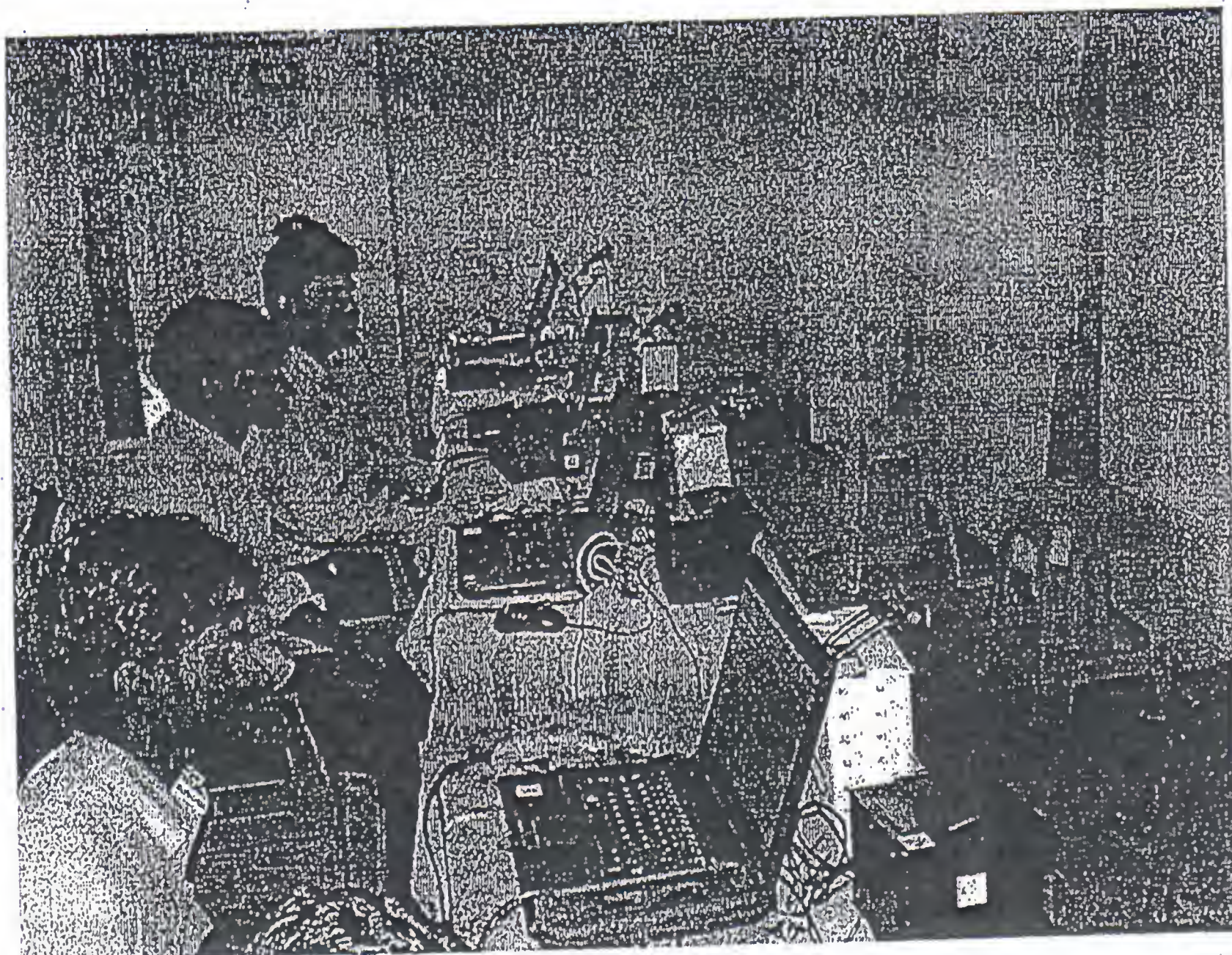


Figure 4 Enrolment stations

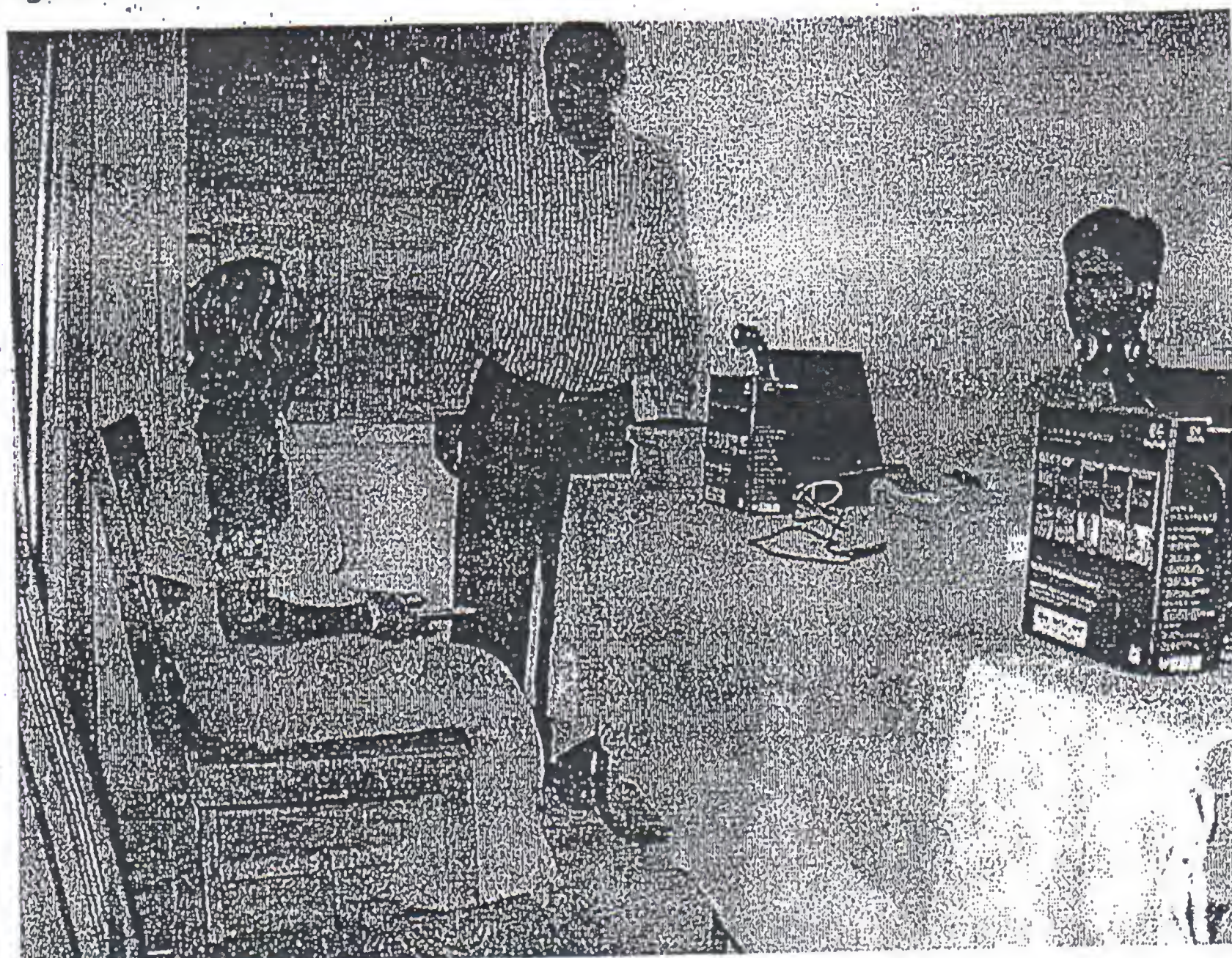


Figure 5 Enrolment station

Enrolment Process

The basic process and associated workflow enforced by the enrolment software is described below. There were minor variations in each state due to the different devices used and the differences in demographic data collection; these variations are listed subsequently.

1. The enrollee would arrive at the enrolling centre with an identifying card. The first station was a non-biometric station where the demographic information of the enrollee was either collected from the card or retrieved from an existing database. A form populated with the demographic information was then printed (or in some cases, forms were printed ahead of time) and any necessary corrections made. The demographic information collected was name, address, date of birth (or age), and occupation.
During the second round of enrolment, the tear-off receipt (described in step 6) was used to identify the application number of the applicant.
Following this the enrollee was sent to an available biometric enrolment station.
2. Using the application number from the application form or first round receipt, the enrollee's demographic record was populated in the enrolment screen. At this point, the operator would check for biometric exceptions (missing fingers or eyes) by asking the enrollee to show his/her hands. If there was an exception, it would be marked in the exception section of the screen, and the information would be stored in the XML file along with the demographic information.
3. Once the above process was completed, the biometric capture would start. The enrollee would first sit down facing the operator and the face photo would be captured by a webcam. The enrolment software would then perform a quality check and crop the image. If the quality check or image cropping failed, the photo would be recaptured up to a maximum of four total attempts. The cropped face photo would be shown on a small frame on the right and it would remain on display during the rest of the biometric capture (see Annexure 1 for screen shots).

A white non-reflecting background screen was placed behind the enrollee's chair to provide a uniform background for face photo capture, and ensure that the background portion of the photo quality check was met. While capturing face photo, the enrollee was instructed to look straight and keep his or her mouth closed.

During the second round of enrolment, the face photo from the first round of enrolment would appear on the application screen so that the operator could confirm that the same person whose biometrics had been captured in the first round was being re-enrolled. After confirming that the photo matched the enrollee, the operator would capture a new face photo which would be cropped, and replace the earlier photo on the screen. The photo would be stored along with the other biometrics in the second round database.

191
265

4. The iris images of the enrollee were captured with a single-eye or two-eye iris capture device. Based on the results of the quality check, the images would be recaptured for a maximum of four total attempts. While capturing iris image, the enrollee was instructed to look straight into the LEDs, rectangle or other appropriate point (depending on the device); open his or her eyes wide ("look angry or glare") and to not blink.
5. The three slap fingerprint images (4-4-2), i.e. left hand slap, right hand slap, and slap image of the two thumbs, were captured. As above, based on the results of the quality check, the capture would be attempted up to four times. The slap fingerprint capture was done with the enrollee standing. This was to ensure that the person could apply sufficient pressure to be able to get good fingerprints. While capturing fingerprint images, the enrollee was instructed to open their hands, place their fingers flat on the platen in the correct position and press their fingers down firmly.
6. Individual fingerprints of all ten fingers were captured using a single-finger capture device. The individual prints were matched with the corresponding prints from the segmented images of the slap fingerprint captured in step 4. If the fingerprints did not match, step 5 was repeated, while still not exceeding a total of four slap attempts for each type of slap capture. This capture was also done with the enrollee standing.
7. If one or more of the enrollee's fingers or eyes were missing, an exception photograph of the enrollee's face along with both hands opened to show the missing fingers would be captured. This was in order to have a visual record of the missing biometrics.
8. In the first round of enrolment, a tear-off receipt that was printed at the bottom of the application form was given to the enrollee, and the enrollee was asked to bring the tear-off receipt when returning for re-enrolment in the second round.



Figure 6 Damaged finger example

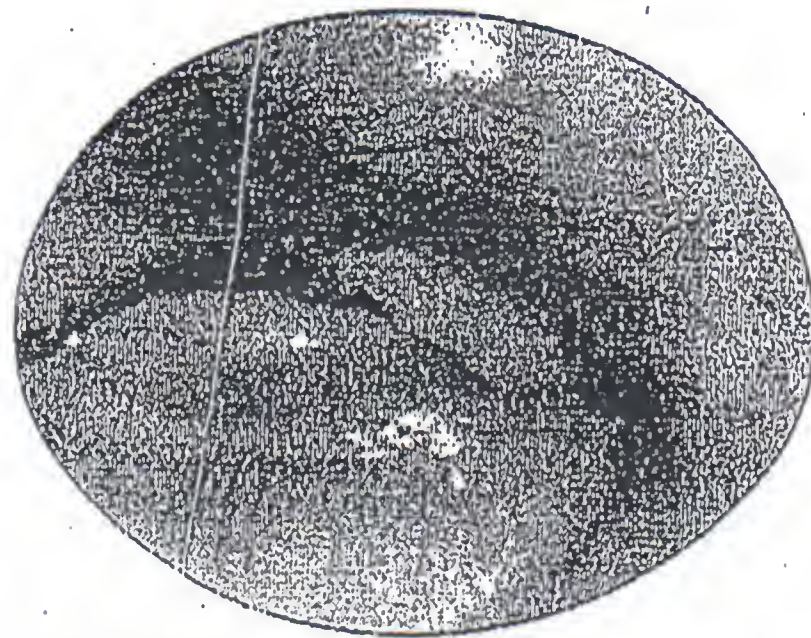


Figure 7 Damaged eye example

192
266

Process Variations

1. Identifying document of enrollee: The enrollee would come to the enrolling centre with his or her ration card in the case of Karnataka and Andhra Pradesh. In Bihar, the enrollee was asked to bring his or her job card. Neither of these cards would completely identify the individual since a single ration card listed all members of the family and each job card would list all adult members of the family. So, an additional digit was appended to the ration card or job card number to create an application number identifying the individual.

Collection of demographic information: In Karnataka, a pre-printed form which had the relevant data for the enrollee was chosen from a stack containing forms for all residents of the village sorted by ration card number. This was handed to the enrollee. In Andhra Pradesh, a form containing the enrollee information was printed at the enrolment site and handed over to the enrollee. In Bihar, the enrollees were asked to fill in the form (if necessary, the enrolment agency employee filled the form for the enrollee) and the data was then entered into the application.

2. For iris capture, there were three variations in the three states:
In Bihar, a binocular type iris capture device was used. Ideally, the enrollees would be able to hold the iris device to their eyes unassisted, and wait for the iris capture to complete. In practice, the operator sometimes helped hold the device up, particularly in the case of older enrollees.

In Andhra Pradesh, the operator held the device. The enrollee would stand up and the operator would bring the capture device close to the enrollee's face and then move the device back slowly to capture the iris image. Both single eye devices and dual eye devices were used. Dual eye device were used for about 61.5 percent of the enrolments and the remaining were done used the single eye device.

In Karnataka, a dual eye device was used and it was mounted on a tripod for a large part of the PoC. The resident would move his or her face slowly towards the device and the device would capture the iris image at the appropriate distance. A small portion of the PoC was done using the iris capture device as a hand-held device, where the operator moved the device towards the enrollee's eyes. The PoC done later in the school in Karnataka also used the same dual eye device as a hand held device.

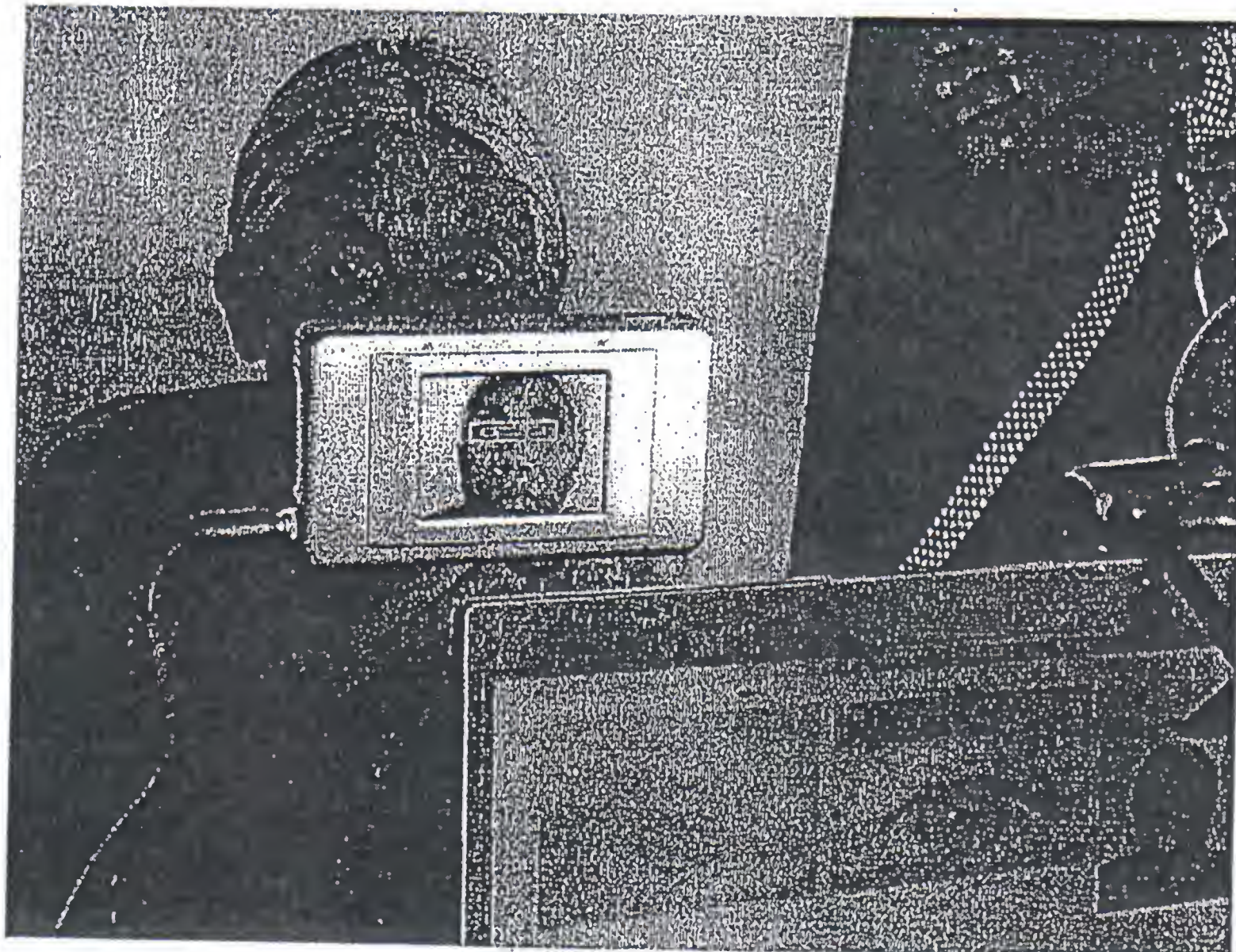


Figure 8: Karnataka- iris camera mounted on a tripod

Enrolment software

The enrolment software had the following screens (Annexure 1)

1. Demographic data and biometric exception capture
2. Face photo capture
3. Dual iris capture
4. Slap fingerprint capture – three slaps to capture all ten fingerprints
5. Capture of ten fingerprints using a single finger device
6. Capture of an exception photograph if necessary

The following are a few noteworthy points related to the enrolment software:

Once the face photo was captured and cropped, it was displayed on a small frame during the capture of all the other biometrics. This would allow the operator to avoid mistakes and avoid combining the biometrics of two different individuals in one enrolment if there was an interruption halfway through the enrolment process.

There were visual biometric quality indicators associated with each image, which the operator could use to quickly gauge image quality (Annexure 1). This was done to avoid the necessity for the operator to interpret quantitative scores.

194
268

The enrolment software would save time stamps during each screen transition, i.e. when moving from one of the screens (1 to 5) listed above to any of the other screens. This was used to measure the "process" time associated with the capture of each biometric. The time measured was not directly related to the time spent by the device to capture the image.

In the context of the UID, the time required for enrolment of each person was a very important factor since it directly translated into the resources needed. Therefore, it was important to record the overall "process" time related to the capture of each biometric and not only the device capture time. For instance, the time measured included the time spent by the operator giving instructions related to the biometric capture, the time spent in the enrollee positioning himself or herself for the specific biometric etc.

Thus, the measured times may not be applicable in a different context. In particular, when the enrollee is experienced in the process and if self-enrolment is done, the conclusions reached here would not be valid. Also, the measurement was not designed to measure device efficiency beyond the UID context.

The "process" timestamps and the number of attempts captured by the software allowed us to compute average capture times and the average number of capture attempts per biometric. In conjunction with the age and occupation captured in the demographic screen, we were also able to analyse the average capture time and average number of capture attempts by age and by occupation. This was important since there are several occupations where repeated rubbing and scratching of fingers result in worn out fingerprints.

Finally the software also indicated the number of fingers and eyes for which images could not be captured in each enrolment, because the corresponding finger or eye was missing or damaged. Even in these cases, the remaining biometrics were captured and the enrolment was completed successfully

Re-enrolment Rates

One of the important goals of the PoC was to create known duplicates by having each enrollee come back after three weeks to be re-enrolled. During the planning of the PoC, there was apprehension that a significant number of enrollees would not come back for re-enrolment. This was a source of concern particularly in Karnataka and Andhra Pradesh, where the PoC was not associated with any ongoing government benefits program and was a standalone experiment. Therefore, incentives were provided for enrollees to re-enrol. In Andhra Pradesh, and Bihar, each enrollee was given seventy rupees following re-enrolment. In Karnataka, a small snack was provided both during the first round and during the second round of enrolment. Despite these efforts, the conservative target rate of re-enrolment was set at eighty percent. Therefore twenty-five thousand people in each state were targeted in the first round to generate matched pair of twenty thousand after the second round. Actual re-enrolment rates were very good and the enrolment agencies were able to reach the targets without much difficulty.

The following are the actual re-enrolment rates observed.

Karnataka Re-enrolment Rates

| | Taluk | Gram Panchayath | Enrolment numbers | Reenrolment numbers | Percentage re-enrolling |
|--------|--------------|-----------------|-------------------|---------------------|-------------------------|
| Tumkur | Tumkur | Bellary | 1,976 | 1,692 | 85% |
| Tumkur | Channarayana | Channarayana | 2,262 | 1,747 | 77% |
| Tumkur | Madhugiri | Doddaballapur | 2,193 | 1,797 | 82% |
| Tumkur | Tiptur | Kibbanahalli | 2,548 | 2,171 | 85% |
| Tumkur | Sirsi | Bullkabana | 2,267 | 1,615 | 71% |
| Mysore | Mysore | Varuna | 2,283 | 2,097 | 92% |
| Mysore | HID Koré | Honnarayana | 2,698 | 2,510 | 93% |
| Mysore | Nanjangud | Hadinaaru | 1,908 | 1,659 | 87% |
| Mysore | Hunsur | Gowdagere | 2,728 | 2,454 | 90% |
| Mysore | KR Nagar | Tippur | 2,754 | 2,331 | 85% |
| | | Karnataka Total | 23,852 | 20,075 | 84% |

Andhra Pradesh Re-enrolment Rates

| District | Mandal | Village | Enrolment numbers | Reenrolment numbers | Percentage re-enrolling |
|----------|-----------------|----------------|-------------------|---------------------|-------------------------|
| Medak | Ilupati | Ghanpur | 2000 | 1819 | 91% |
| | Wargal | Wargal | 2435 | 2123 | 87% |
| | Wargal | Veluri | 2095 | 1978 | 94% |
| | Chegunta | Narsingi | 2756 | 2539 | 92% |
| | Patancheru | Ward-11 | 2602 | 1187 | 46% |
| Krishna | Mylavaram | Yelvadam | 2326 | 2477 | 88% |
| | Kanikavaram | Lakshminipalam | 2481 | 2169 | 87% |
| | Mylavada Rural | Nidamanuru | 3033 | 2669 | 88% |
| | Penamaluru | Poranki | 3114 | 2532 | 81% |
| | Yajaywada Urban | Ward-9 | 2377 | 1200 | 50% |
| | | AP Total | 25717 | 20683 | 80% |

196
270

Observations

The following are the observed average capture times and number of attempts

| | | Face photo | Iris | Slap Fingerprints (three images) |
|--------------------------|---|------------|------------|----------------------------------|
| Adults | Capture times (for all attempts combined) | 34 seconds | 52 seconds | 1 minute 51 seconds |
| Adults | Number of attempts | 1.5 | 1.9 | 1.5 |
| Children (4 to 15 years) | Capture times (for all attempts combined) | 33 seconds | 55 seconds | 1 minute 13 seconds |
| Children (4 to 15 years) | Number of attempts | 1.4 | 3.1 | 1.4 |

The important process time averages are as shown below:

Average biometric enrolment time for adults is 3 minutes 17 seconds

Average biometric enrolment time for children (4 to 15 years) is 2 minutes 21 seconds

Capture times analyzed by age, occupation, and gender are listed in Annexure 2

| | Percentage of enrollees |
|---|-------------------------|
| One or more fingers missing or otherwise not capturable | 1.2% |
| Either or both eyes missing or otherwise not capturable | 0.5% |
| Missing all 10 finger and both eyes | 0.012% |

Table: Biometric Exceptions (missing eyes and fingers)

The average time required for capture of face photo, fingerprints of ten fingers and iris image of adults was three minutes and seventeen seconds. Of this, a little over half the time was spent on fingerprint capture. The time for iris capture was a little below one minute, and face photo capture took over half a minute. The iris image capture time varied significantly by age, with people above eighty taking twice as long as people in their twenties. The variation in capture time of fingerprints was lower with the older group taking twenty percent longer than the younger group. One apparent anomaly in fingerprint capture times is that 20 to 30 year old people took longer to have their fingerprint captured than older people. This can possibly be attributed to the fact that they may be engaged in occupations involving heavier physical labour and correspondingly more wear on their fingerprints than their older

197
278

counterparts. The average capture time for iris images and fingerprints for children were no worse than that for adults. This included the youngest children who were only four years old.

The enrolment time also showed significant variation by occupation, with the occupations involving physical labour showing longer enrolment times. For example, agricultural labourers took about one-third longer to have their fingerprints captured compared with public and private sector employees and other white collar workers. Similarly, for iris capture, the variation was over thirty percent.

There were many blind people who had their iris captured successfully. This was because even though they were blind, their iris was intact. Similarly, many people with worn fingerprints had their fingerprints successfully captured. The table above shows that the percentage of residents enrolled with one or more missing fingers was only a little over one percent and the percentage of enrollees with one or both eyes missing was less than one percent of the total enrollee population.

The enrolment PoC for children showed that the process of enrolling children in the age range of four to fifteen was not significantly harder than that of enrolling adults.

Process observations

An important conclusion reached was that the best possible way for conducting biometric enrolment was to have the enrollee be stationary and have the operator do the positioning of the device.

It was also clear that the operator instructions to the resident were very important. The best results obtained in terms of quality and efficiency was when the operator spent a few seconds *ahead of* each biometric capture clearly explaining what was required on the part of the enrollee, for example "keep eyes wide open", "keep fingers flat on the platen and press hard", etc. This was much more effective than trying to correct the enrollee's gaze, positioning etc. *during* the capture of the biometric.

The use of quality check software clearly helped in two ways. The first was that there was a clear message that quality of data collected mattered to the UIDAI and that the quality was going to be monitored. The second was that the operator began to recognize good quality images and over time was well versed in collecting high quality images.

The physical layout of the devices and the ability of the operator to reach out and help the enrollee as required were also seen to be important. Therefore the width of the table had to be small enough so that the operator could reach across. The other option was that the enrollee stood next to the operator on the right side for fingerprint capture.

The ambient light was not always sufficient to capture good quality face photographs even during the day. Table lamps or other artificial lighting was often needed.

The mobile USB tethered iris devices used were adequate for capturing good quality images. In addition, fingerprint images from different devices were matched and there were no

198
282

compatibility issues in doing the matching. In general, the devices worked as expected. The differences in process were much more significant compared to the differences in devices.

Iris enrolment was eminently possible from the operator's perspective and was also well accepted by the enrollee. In fact, the iris capture took less time than fingerprint capture.

Older people sometimes needed assistance in positioning themselves (see picture below) and often required assistance in pressing their fingers hard enough on the platen to get good fingerprints. Children were able to position themselves correctly and maintain the position long enough for successful capture of all three biometrics.

The PoC was conducted in the summer months of April, May and June in Medak district of Andhra Pradesh and in Nalanda district in Bihar. During a few days when the PoC was in progress, the temperature reached 44 degrees Celsius in Nalanda district. Despite the extreme temperature and the fact that no fans were available, enrolment went on normally.

In conclusion, it is clear that it is possible to collect good quality biometrics in rural India despite existing shortages in infrastructure, and the biometric variations within the rural population. Reasonable processes can be specified to undertake enrolment on a much larger scale



Figure 9: Older resident being assisted with slap fingerprint capture

199
283

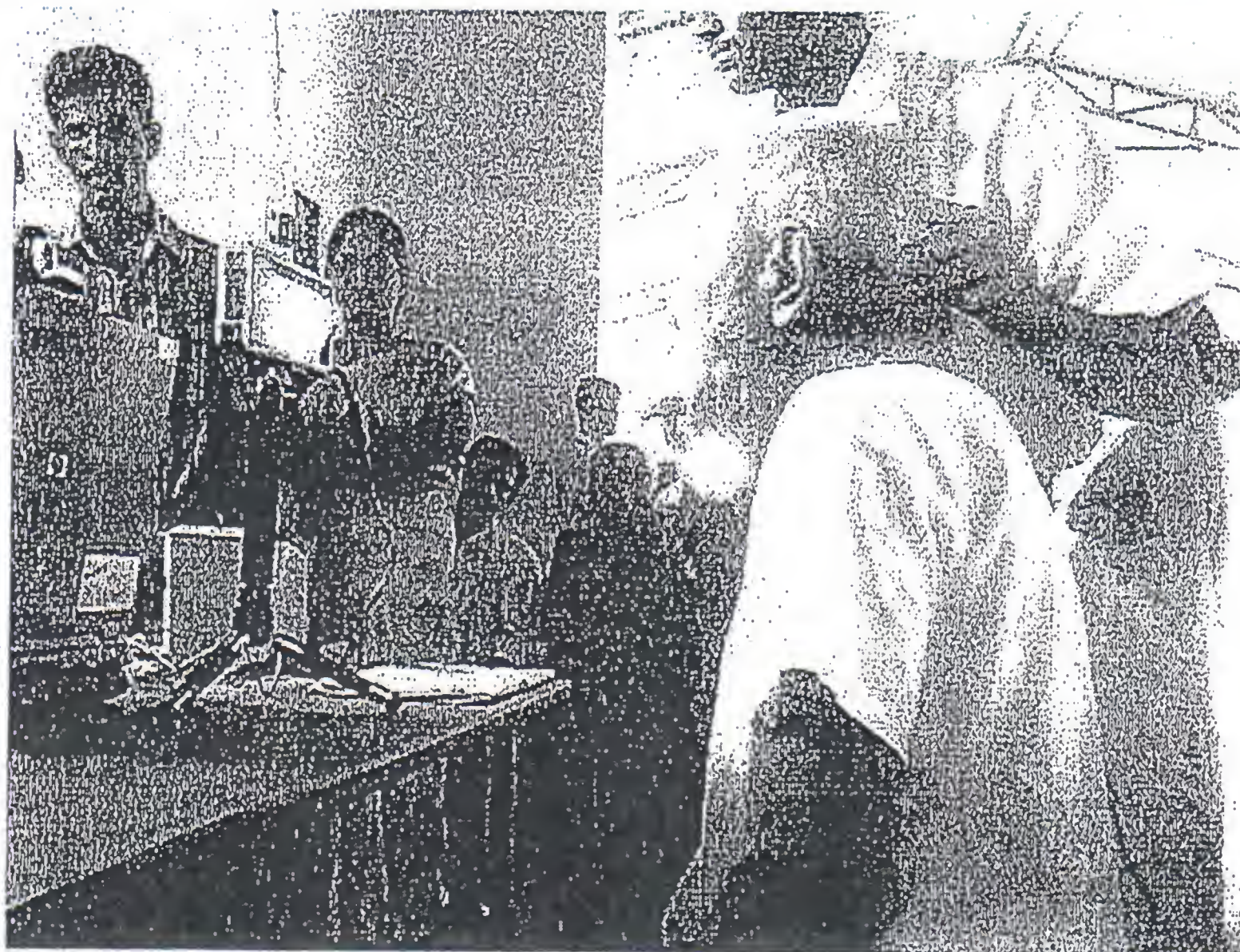


Figure 10: Eighty six year old resident being assisted with iris capture

Biometric observations

The ultimate goals of biometric enrolment for the UIDAI are two-fold. One is to carry out biometric deduplication for all enrollees in India, and the second is to authenticate the biometrics of an enrolled resident on demand. Therefore, these activities have been the focus of the analysis conducted on the PoC data.

Biometric matchability analysis was done on the PoC data to understand the quality of the data and how well it could be used for deduplication and authentication. The basic tool used to study the results is the ROC (Receiver Operational Curve) which shows how two types of potential errors can be traded off against each other for the given set of data. Two of the ROC curves that were obtained from the analysis are shown in Annexure 3 to show a sample of the analysis and to explain the results. The analysis was done using images of ten fingerprints and two irises. The face biometric was not used for matching.

Terminology

The following terminology is needed to understand the results.

Identification: This is the process where any one person's biometrics is matched with that of *all* the other people in the database. This results in establishing the enrollee's biometrics as either unique or as a likely duplicate of the biometrics of an enrollee who had enrolled earlier.

200
274

FPIR: False Positive Identification Rate: This is the likelihood that a person's biometrics is seen as a duplicate (i.e., the biometric deduplication software identifies his biometrics as matching with that of a different person), even though it is not a duplicate in reality.

FNIR: False Negative Identification Rate: This is the likelihood that a person enrolls a second time and the deduplication software is unable to identify their biometrics as a duplicate set.

Verification: This is the process where a person's biometrics is compared only with a copy of his or her biometrics that was captured earlier.

FAR: False Accept Rate: This is the likelihood that a person's biometrics is matched against a different person and the biometrics is seen to match, i.e. the person is wrongly seen to be a different person.

FRR: False Reject Rate: This is the likelihood that a person's biometrics does not match against an earlier sample of his or her biometrics and so he or she is not recognized as the same person.

Results

The matching analysis was done on two sets of 20,000 biometrics, for a total of 40,000. However, the number of comparisons was several orders of magnitude more than 40,000, since each set of fingerprints would be matched against every other set of fingerprints in the data set. Similarly, the iris images from each person would be matched against that of every other person in the data set. Therefore, the results are statistically significant and can be extended to larger populations.

We will now compile the data on the accuracy obtained by enrolling with only fingerprints, enrolling with only iris images, and by enrolling with both biometrics. We will do so using the Identification ROC curve shown in Appendix 3. To compare the accuracies in these three cases, we will look at the point where the FPIR (i.e. the possibility that a person is mistaken to be a different person) is 0.0025 %.

Comparing the FNIR numbers achieved, the FNIR using two irises only is 0.5%, that achieved by using ten fingers only is 0.25%, and that achieved by using ten fingers and two irises is 0.01%. The conclusion we can draw is that accuracy achievable using ten fingerprints is twice that of the accuracy achieved using iris images. Even more important, the accuracy achieved by using ten fingerprints and two irises is fifty times better than by using irises alone and twenty five times better than by using fingerprints alone. The accuracy level achieved was 99.99% in this case.

Looking at the verification ROC for children and adults, we can see that the accuracy obtained in matching for children using iris is better than that for adults. Similarly, the accuracy obtained using fingerprints is better for children than for adults..

By doing analysis as shown in the examples above on real data captured under typical Indian conditions in rural India, we can be confident that biometric matching can be used on a wider

scale to realize the goal of creating unique identities. We have further confirmed that is true as much for children as for adults.

Conclusion

The PoC study was a useful precursor to large scale UID enrolment and has validated our hypotheses regarding biometric enrolment. Iris enrolment was not particularly difficult, and dramatically improved the accuracy levels that could be achieved. The biometric accuracy levels necessary for deduplication of all residents of India are achievable. The time needed for capture of biometrics in typical rural conditions is small enough to support large scale enrolment. In conclusion, the PoC study was a productive part of the ongoing rollout of the UID program.

202
27/6

Annexure 1 - Enrolment application screen shots

Demographic screen with exception indicators

UID PoC Enrollment Reference Implementation Ver 1.1 RC03

Fields Marked as * are mandatory

English

Application Number: * Enrollment ID: *

Name: *

DB Type: ☐ Verified ☐ Declared ☐ Approximate *

Date of Birth: **

Gender: ☐ Male ☐ Female ☐ TG *

Building: *

Street: *

LandMark: *

Locality: *

Village: *

Taluka: *

District: *

State: *

Country: *

PIN: *

Occupation: *

Others: *

Guardian Name: *

Relationship: ☐ Father ☐ Mother ☐ Guardian ☐ Not Given

Guardian Unique ID: *

Verification: ☐ Document ☐ Community ☐ Introducer

Introducer Name: *

Introducer Unique ID: *

Mobile No: *

Email: *

Local Language

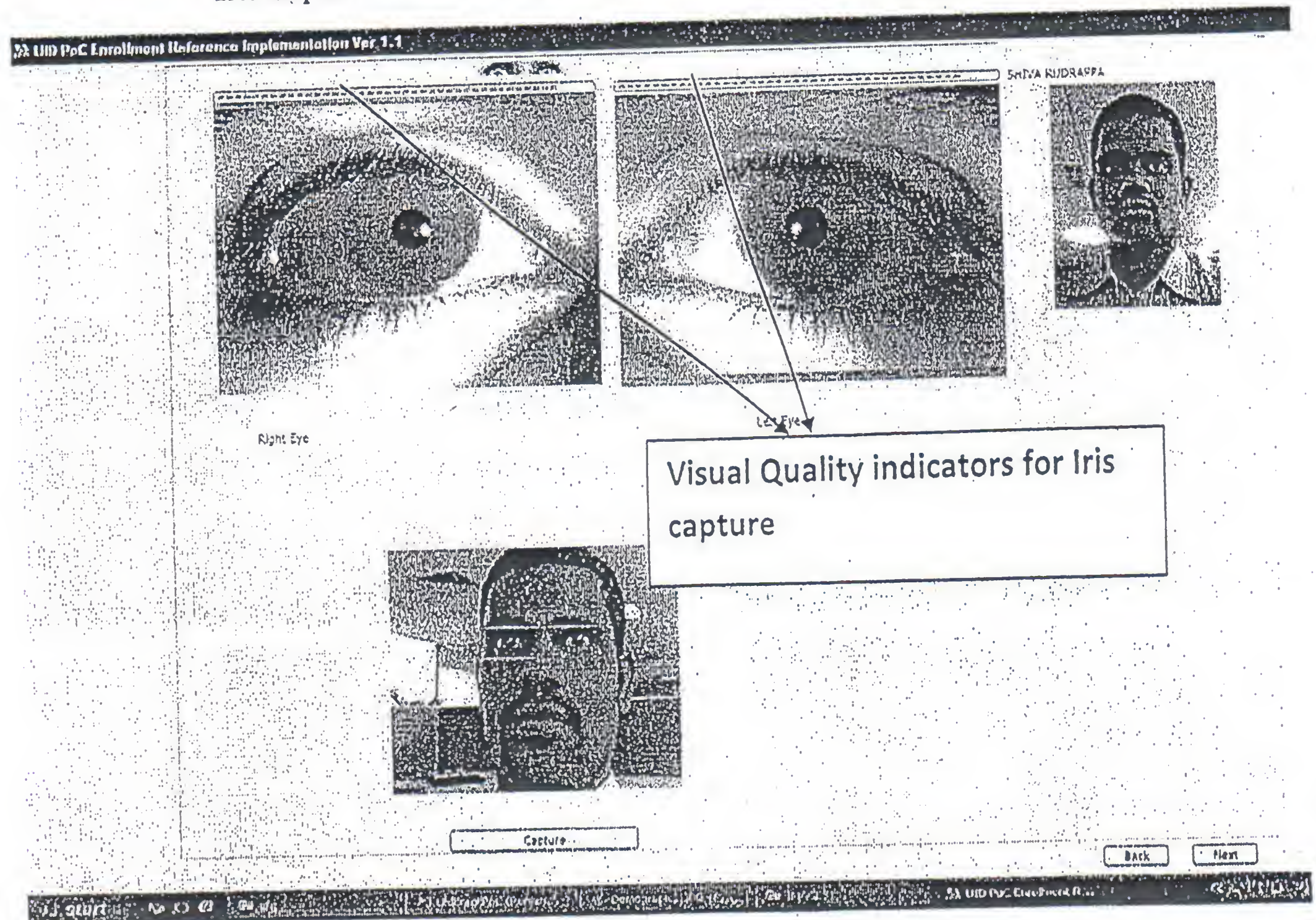
Missing Finger Indication: *

Missing Eye Indication: *

Clear Data Next

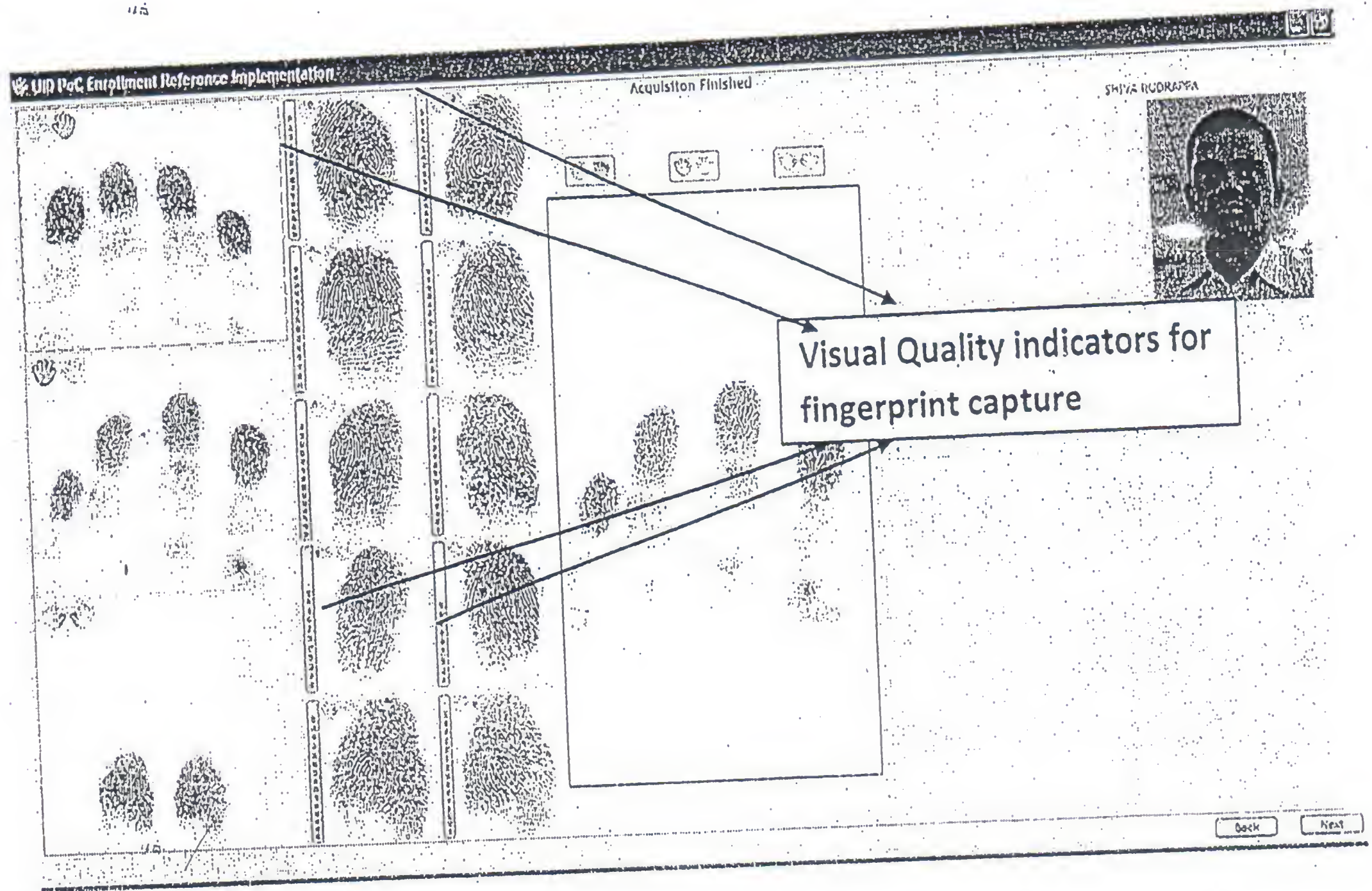
203
277

Iris Capture Screen with quality indicators highlighted



204
278

Fingerprint Capture Screen with quality indicators highlighted



205
279

Single Fingerprint Capture Screen



Annexure 2 - Enrolment times by age and demographics

| Age | Under 20 | 20 to 30 | 30 to 40 | 40 to 50 | 50 to 60 | 60 to 70 | 70 to 80 | Above 80 |
|------|----------|----------|----------|----------|----------|----------|----------|----------|
| Face | 0:00:31 | 0:00:31 | 0:00:33 | 0:00:35 | 0:00:37 | 0:00:38 | 0:00:40 | 0:00:45 |
| iris | 0:00:42 | 0:00:42 | 0:00:49 | 0:00:54 | 0:00:58 | 0:01:07 | 0:01:15 | 0:01:24 |
| slap | 0:01:45 | 0:01:52 | 0:01:42 | 0:01:45 | 0:01:53 | 0:01:55 | 0:02:08 | 0:02:14 |

Enrolment times by age

| Occupation | face | iris | slap | Total |
|--------------------|---------|---------|---------|---------|
| Agriculture Labour | 0:00:27 | 0:00:53 | 0:02:11 | 0:03:31 |
| Employee | 0:00:27 | 0:00:39 | 0:01:36 | 0:02:43 |
| Daily wage earner | 0:00:25 | 0:00:46 | 0:02:03 | 0:03:14 |
| Student | 0:00:22 | 0:00:37 | 0:01:49 | 0:02:49 |
| House Wife | 0:00:27 | 0:00:59 | 0:02:04 | 0:03:29 |
| Coolie | 0:00:55 | 0:00:48 | 0:01:28 | 0:03:11 |
| Handicraft | 0:00:43 | 0:00:51 | 0:01:41 | 0:03:15 |
| Beedi Worker | 0:00:21 | 0:00:41 | 0:02:37 | 0:03:02 |
| Artisan | 0:00:22 | 0:00:42 | 0:03:20 | 0:04:24 |
| Driver | 0:00:33 | 0:00:39 | 0:01:52 | 0:03:04 |
| Other | 0:00:27 | 0:00:44 | 0:02:16 | 0:03:27 |
| Retired | 0:00:28 | 0:01:40 | 0:02:08 | 0:04:16 |
| Rickshaw Puller | 0:00:24 | 0:00:37 | 0:01:24 | 0:02:35 |

Enrolment times by occupation

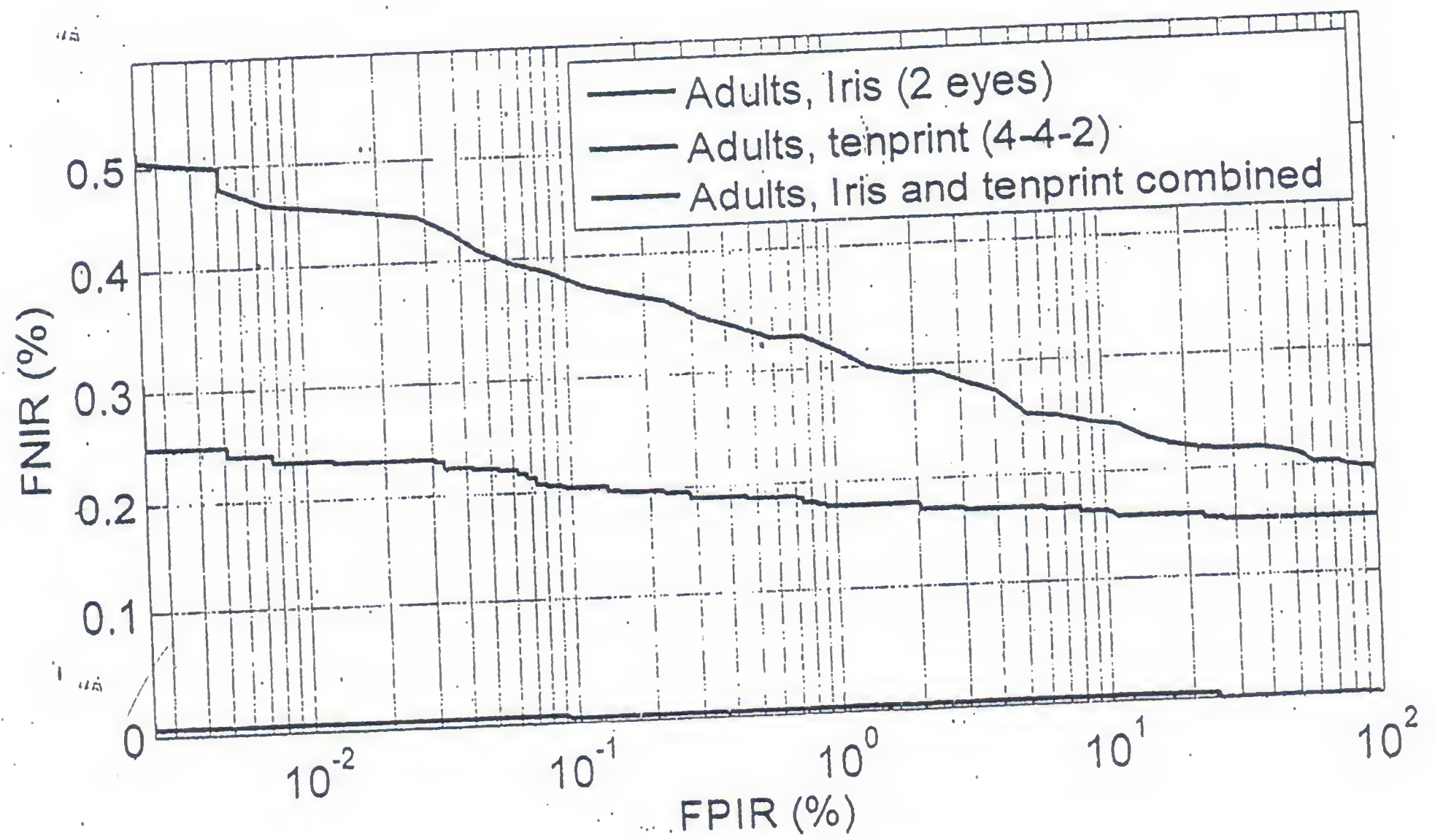
| | face | iris | slap | total |
|--------|---------|---------|---------|---------|
| Male | 0:00:30 | 0:00:48 | 0:01:50 | 0:03:08 |
| Female | 0:00:27 | 0:00:56 | 0:02:09 | 0:03:32 |

Enrolment times by gender

207
281

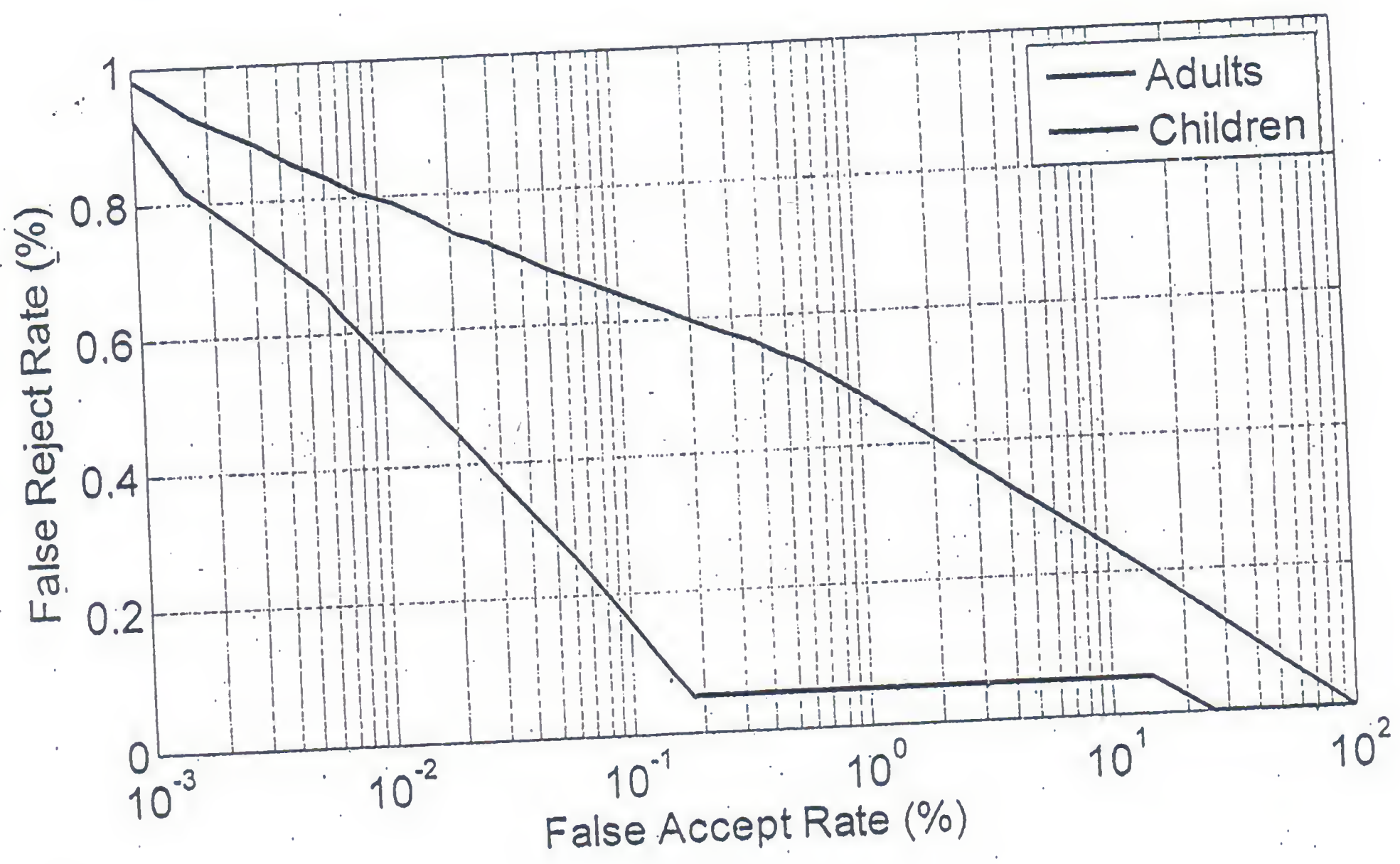
Annexure 3 – Biometric matching accuracy curves

Identification ROCs(1 in 20,000) for adults



208
282

Iris identification ROCs (1:1) for adults and children



283

Verification ROC for 1,000 children and adults

